ESET ENDPOINT SECURITY

Guida dell'utente

Microsoft® Windows® 8 / 7 / Vista / XP / 2000 / Home Server

Fare clic qui per scaricare la versione più recente di questo documento

ESET **ENDPOINT SECURITY**

Copyright ©2013 di ESET, spol. s r. o.
ESET Endpoint Security è stato sviluppato da ESET, spol. s r. o.
Per ulteriori informazioni, visitare il sito Web www.nod32.it.
Tutti i diritti riservati. Sono vietate la riproduzione, l'archiviazione in sistemi di registrazione o la trasmissione in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, tramite fotocopia, registrazione, scansione o altro della presente documentazione in assenza di autorizzazione scritta dell'autore.
ESET, spol. s r. o. si riserva il diritto di modificare qualsiasi parte dell'applicazione software descritta senza alcun preavviso.

Assistenza clienti nel mondo: www.nod32.it/support

REV. 20. 2. 2013

Contenuti

1. ESET Endpoint Security 5

1.1 Requisiti di sistema 5
1.2 Prevenzione 5

2. Installazione 7

2.1 Installazione tipica 8
2.2 Installazione personalizzata 10
2.3 Inserimento di nome utente e password 14
2.4 Aggiornamento ad una versione più recente 14
2.5 Controllo computer 15

3. Guida introduttiva 16

3.1 Introduzione all'interfaccia utente 16
3.2 Cosa fare se il programma non funziona correttamente 17
3.3 Configurazione dell'aggiornamento 18
3.4 Configurazione del server proxy 19
3.5 Impostazione protezione 20
3.6 Configurazione area sicura 21

4. Utilizzo di ESET Endpoint Security 22

4.1 Computer 24
4.1.1 Protezione antivirus e antispyware 24
4.1.1.1 Protezione file system in tempo reale 25
4.1.1.1.1 Supporti da controllare 25
4.1.1.1.2 Controllo al verificarsi di un evento 26
4.1.1.1.3 Opzioni avanzate di controllo 26
4.1.1.1.4 Livelli di pulizia 26
4.1.1.1.5 Quando modificare la configurazione della protezione in tempo reale 27
4.1.1.1.6 Controllo della protezione in tempo reale 27
4.1.1.1.7 Cosa fare se la protezione in tempo reale non funziona 27
4.1.1.2 Protezione documenti 28
4.1.1.3 Controllo computer 28
4.1.1.3.1 Tipo di controllo 29
4.1.1.3.1.1 Controllo intelligente 29
4.1.1.3.1.2 Controllo personalizzato 29
4.1.1.3.2 Oggetti da controllare 29
4.1.1.3.3 Profili di controllo 30
4.1.1.3.4 Avanzamento controllo 30
4.1.1.4 Controllo all'avvio 31
4.1.1.4.1 Controllo automatico file di avvio 31
4.1.1.5 Esclusioni dal percorso 32
4.1.1.6 Configurazione parametri motore ThreatSense 33
4.1.1.6.1 Oggetti 33
4.1.1.6.2 Opzioni 34
4.1.1.6.3 Pulizia 34
4.1.1.6.4 Estensione 35
4.1.1.6.5 Limiti 35
4.1.1.6.6 Altro 36
4.1.1.7 Rilevamento di un'infiltrazione 36
4.1.2 Supporti rimovibili 38
4.1.3 Controllo dispositivi 38
4.1.3.1 Regole controllo dispositivi 39
4.1.3.2 Aggiunta di regole controllo dispositivi 40
4.1.4 Sistema anti-intrusione basato su host (HIPS) 41

4.2 Rete 43
4.2.1 Modalità di filtraggio 44
4.2.2 Profili firewall 45
4.2.3 Configurazione e uso delle regole 46
4.2.3.1 Configurazione delle regole 47
4.2.3.2 Modifica delle regole 48
4.2.4 Configurazione aree 49
4.2.4.1 Autenticazione di rete 49
4.2.4.1.1 Autenticazione area - Configurazione client 49
4.2.4.1.2 Autenticazione area - Configurazione server 51
4.2.5 Stabilire la connessione - rilevamento 52
4.2.6 Registrazione 53
4.2.7 Integrazione nel sistema 53

4.3 Web ed e-mail 54
4.3.1 Protezione accesso Web 55
4.3.1.1 HTTP, HTTPS 55
4.3.1.1.1 Modalità attiva per i browser Internet 56
4.3.1.2 Gestione indirizzo URL 56
4.3.2 Protezione client di posta 57
4.3.2.1 Filtro POP3, POP3S 58
4.3.2.2 Controllo protocolli IMAP, IMAPS 59
4.3.2.3 Integrazione con client di posta 59
4.3.2.3.1 Configurazione della protezione client di posta 60
4.3.2.4 Eliminazione delle infiltrazioni 61
4.3.3 Protezione antispam 61
4.3.3.1 Aggiunta di indirizzi alla whitelist e alla blacklist 62
4.3.3.2 Contrassegnare messaggi come spam 62
4.3.4 Filtraggio protocolli 63
4.3.4.1 Web e client di posta 63
4.3.4.2 Applicazioni escluse 64
4.3.4.3 Indirizzi IP esclusi 65
4.3.4.3.1 Aggiungi indirizzo IPv4 65
4.3.4.3.2 Aggiungi indirizzo IPv6 65
4.3.4.4 Verifica protocollo SSL 66
4.3.4.4.1 Certificati 66
4.3.4.4.1.1 Certificati attendibili 66
4.3.4.4.1.2 Certificati esclusi 67
4.3.4.4.1.3 Comunicazioni SSL crittografate 67

4.4 Controllo Web 68
4.4.1 Regole del controllo Web 68
4.4.2 Aggiunta di regole del controllo Web 69
4.4.3 Editor gruppi 70

4.5 Aggiornamento del programma 70
4.5.1 Configurazione dell'aggiornamento 74
4.5.1.1 Aggiorna profili 75
4.5.1.2 Configurazione aggiornamento avanzata 75
4.5.1.2.1 Modalità di aggiornamento 75
4.5.1.2.2 Server proxy 76
4.5.1.2.3 Connessione alla LAN 76
4.5.1.2.4 Creazione di copie di aggiornamento - Mirror 77
4.5.1.2.4.1 Aggiornamento dal Mirror 78
4.5.1.2.4.2 Risoluzione dei problemi di aggiornamento Mirror 79
4.5.1.3 Annullamento aggiornamento 80
4.5.2 Come creare attività di aggiornamento 81

4.6 Strumenti 82
4.6.1 File di rapporto 83
4.6.1.1 Manutenzione rapporto 84
4.6.2 Pianificazione attività 85
4.6.2.1 Creazione di nuove attività 87
4.6.3 Statistiche di protezione 88

4.6.4 Attività di verifica....89
4.6.5 ESET SysInspector....90
4.6.6 ESET Live Grid....90
4.6.6.1 File sospetti....91
4.6.7 Processi in esecuzione....92
4.6.8 Connessioni di rete....93
4.6.9 Quarantena....95
4.6.10 Invio di file per l'analisi....96
4.6.11 Avvisi e notifiche....97
4.6.11.1 Formato dei messaggi....98
4.6.12 Aggiornamenti del sistema....98
4.6.13 Diagnostica....98
4.6.14 Licenze....99
4.6.15 Amministrazione remota....100
4.7 Interfaccia utente....101
4.7.1 Grafica....101
4.7.2 Avvisi e notifiche....102
4.7.2.1 Configurazione avanzata....103
4.7.3 Finestre di notifica nascoste....103
4.7.4 Configurazione dell'accesso....104
4.7.5 Menu del programma....105
4.7.6 Menu contestuale....106
4.7.7 Modalità Presentazione....106
5. Utente avanzato....108
5.1 Configurazione del server proxy....108
5.2 Importa ed esporta impostazioni....108
5.3 Tasti di scelta rapida....109
5.4 Riga di comando....109
5.5 ESET SysInspector....111
5.5.1 Introduzione a ESET SysInspector....111
5.5.1.1 Avvio di ESET SysInspector....111
5.5.2 Interfaccia utente e utilizzo dell'applicazione....112
5.5.2.1 Comandi del programma....112
5.5.2.2 Navigare in ESET SysInspector....113
5.5.2.2.1 Tasti di scelta rapida....114
5.5.2.3 Confronta....116
5.5.3 Parametri della riga di comando....117
5.5.4 Script di servizio....117
5.5.4.1 Generazione dello script di servizio....117
5.5.4.2 Struttura dello script di servizio....118
5.5.4.3 Esecuzione degli script di servizio....120
5.5.5 Domande frequenti....120
5.5.6 ESET SysInspector come componente di ESET Endpoint Security....122
5.6 ESET SysRescue....122
5.6.1 Requisiti minimi....122
5.6.2 Come creare un CD di ripristino....123
5.6.3 Selezione delle destinazioni....123
5.6.4 Impostazioni....123
5.6.4.1 Cartelle....123
5.6.4.2 Antivirus ESET....124
5.6.4.3 Impostazioni avanzate....124
5.6.4.4 Protocollo Internet....124
5.6.4.5 Supporto USB di avvio....124
5.6.4.6 Masterizza....125
5.6.5 Utilizzo di ESET SysRescue....125
5.6.5.1 Utilizzo di ESET SysRescue....125
6. Glossario....126
6.1 Tipi di infiltrazioni....126
6.1.1 Virus....126
6.1.2 Worm....126
6.1.3 Trojan horse....126
6.1.4 Rootkit....127
6.1.5 Adware....127
6.1.6 Spyware....127
6.1.7 Applicazioni potenzialmente pericolose....128
6.1.8 Applicazioni potenzialmente indesiderate....128
6.2 Tipi di attacchi remoti....128
6.2.1 Attacchi DoS (Denial of Service)....128
6.2.2 Poisoning del DNS....128
6.2.3 Attacchi worm....128
6.2.4 Controllo porta....129
6.2.5 Desincronizzazione TCP....129
6.2.6 SMB Relay....129
6.2.7 Attacchi ICMP....129
6.3 E-mail....130
6.3.1 Pubblicità....130
6.3.2 Hoax: truffe e bufale....130
6.3.3 Phishing....131
6.3.4 Riconoscimento messaggi spam....131
6.3.4.1 Regole....131
6.3.4.2 Whitelist....132
6.3.4.3 Blacklist....132
6.3.4.4 Controllo lato server....132

1. ESET Endpoint Security

ESET Endpoint Security rappresenta un nuovo approccio alla protezione integrata del computer. La versione più recente del motore di scansione ThreatSense ®, associata ai moduli personalizzati del Firewall e antispam, sfrutta la velocità e la precisione per mantenere il computer protetto. Il risultato è un sistema intelligente che rileva continuamente attacchi e software dannoso che minacciano il computer.

ESET Endpoint Security è una soluzione di sicurezza completa nata dall'impegno continuo ad associare massime prestazioni a minimo impatto sul sistema. Le avanzate tecnologie, basate sull'intelligenza artificiale, sono in grado di eliminare in modo proattivo l'infiltrazione da parte di virus, spyware, trojan horse, worm, adware, rootkit e altri attacchi Internet senza ripercussioni sulle prestazioni del sistema o interruzioni del computer.

ESET Endpoint Security è progettato per essere utilizzato principalmente su workstation in un ambiente aziendale/piccole imprese. Può essere utilizzato insieme a ESET Remote Administrator, consentendo di gestire facilmente qualsiasi numero di workstation client, applicare criteri e regole, monitorare i rilevamenti ed eseguire la configurazione remota da qualsiasi computer collegato in rete.

1.1 Requisiti di sistema

Per il corretto funzionamento di ESET Endpoint Security , il sistema deve soddisfare i seguenti requisiti hardware e software:

Microsoft® Windows® 2000, XP

400 MHz 32 bit (x86)/64 bit (x64)
128 MB di memoria di sistema (RAM)
320 MB di spazio disponibile
Super VGA (800 x 600)

Microsoft® Windows® 8, 7, Vista, Home Server

1 GHz 32 bit (x86)/64 bit (x64)
512 MB di memoria di sistema (RAM)
320 MB di spazio disponibile
Super VGA (800 x 600)

1.2 Prevenzione

Quando si utilizza il computer, e in particolare quando si naviga in Internet, occorre tenere presente che nessun antivirus può eliminare completamente il rischio causato da infiltrazioni e attacchi. Per garantire la massima protezione, è essenziale utilizzare correttamente il sistema antivirus e attenersi ad alcune regole utili.

Eseguire regolarmente l'aggiornamento

In base alle statistiche ottenute da ESET Live Grid, ogni giorno vengono create migliaia di infiltrazioni nuove e uniche per aggirare le misure di sicurezza esistenti e generare profitti per i rispettivi autori, a spese e discapito di altri utenti. Gli specialisti dei laboratori antivirus ESET analizzano queste minacce su base giornaliera e preparano e rilasciano gli aggiornamenti per migliorare costantemente il livello di protezione per gli utenti del programma antivirus. Un aggiornamento configurato in modo non corretto riduce l'efficacia del programma. Per ulteriori informazioni su come configurare gli aggiornamenti, consultare il capitolo Impostazione dell'aggiornamento.

Scaricare le patch di protezione

Gli autori di software dannoso preferiscono sfruttare le vulnerabilità dei sistemi per aumentare l'efficacia della diffusione di codice dannoso. Per tale motivo, le società di software esaminano attentamente le nuove vulnerabilità nelle applicazioni create e rilasciano regolarmente gli aggiornamenti di protezione allo scopo di eliminare le potenziali minacce. È importante scaricare questi aggiornamenti della protezione non appena vengono rilasciati. Esempi di tali applicazioni includono il sistema operativo Windows o il browser Internet Explorer ampiamente utilizzato.

Eseguire il backup dei dati importanti

Di norma, gli autori di malware non sono interessati alle esigenze degli utenti e l'attività dei programmi dannosi comporta spesso un malfunzionamento generale del sistema operativo e il danneggiamento volontario di dati importanti. È importante eseguire un backup periodico dei dati importanti e sensibili su un supporto esterno, ad

esempio un DVD o un'unità hard disk esterna. Tali precauzioni consentono di recuperare i dati in modo semplice e rapido in caso di errore del sistema.

Eseguire regolarmente la scansione antivirus

Un controllo automatico e periodico del computer con le impostazioni appropriate consente di rimuovere le infiltrazioni che potrebbero non essere state rilevate a causa della presenza di aggiornamenti delle firme antivirali obsoleti.

Seguire le regole di protezione di base

Questa è la regola più utile e più efficace di tutte: essere sempre prudenti. Oggi, molte infiltrazioni richiedono l'intervento dell'utente affinché possano essere eseguite e distribuite. Se si è prudenti quando si aprono nuovi file, sarà possibile risparmiare tempo e fatica per l'eventuale disinfezione delle infiltrazioni nel computer. Alcune regole utili:

- Non visitare siti Web sospetti, con molte finestre popup e pubblicità che attirano l'attenzione.
- Prestare attenzione durante l'installazione di programmi freeware, pacchetti codec e così via. Utilizzare solo programmi sicuri e visitare solo siti Web Internet sicuri.
- Essere prudenti quando si aprono gli allegati e-mail, in particolare quelli inviati da programmi massmailer a destinatari multipli e quelli inviati da mittenti sconosciuti
- Non utilizzare un account Amministratore per eseguire le attività quotidiane sul computer.

2. Installazione

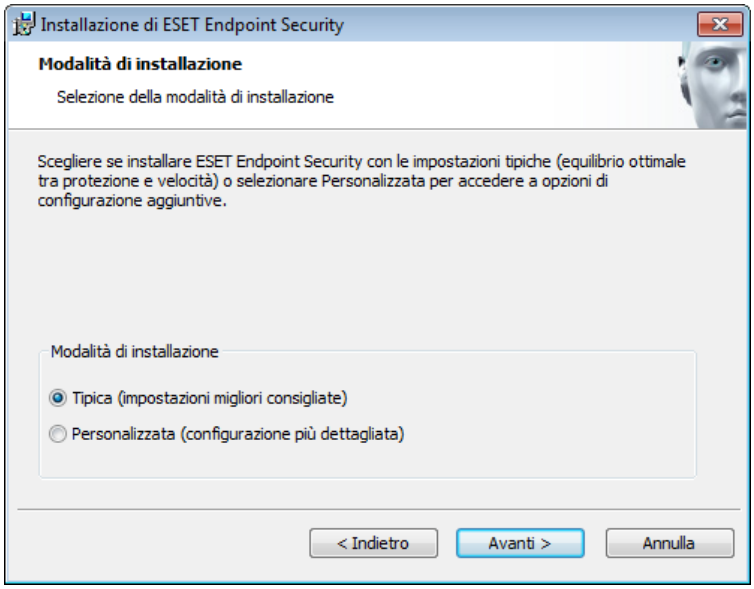
Dopo aver avviato il programma di installazione, l'installazione guidata condurrà l'utente attraverso le fasi dell'impostazione.

Importante: assicurarsi che nel computer non siano installati altri programmi antivirus. Se su un singolo computer sono installate due o più soluzioni antivirus, potrebbero entrare in conflitto tra loro. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema. Per un elenco degli strumenti di disinstallazione dei software antivirus comuni, consultare l'articolo della Knowledge Base ESET (disponibile in inglese e in altre lingue).

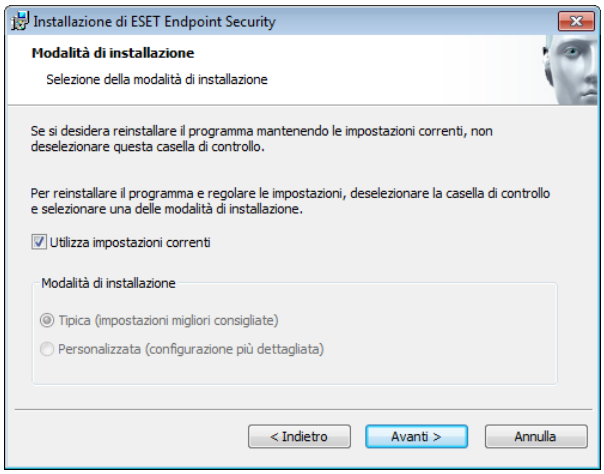
Installazione di ESET Endpoint Security
ESET
ENDPOINT
SECURITY
Benvenuti alla Procedura di Installazione di ESET Endpoint Security
La Procedura di Installazione consentirà di modificare le funzionalità di ESET Endpoint Security installate sul computer o anche di rimuovere ESET Endpoint Security dal computer. Fare clic su Avanti per continuare o Annulla per uscire dalla Procedura di Installazione.
< Indietro
Avanti >
Annulla

Il programma controlla innanzitutto se è disponibile una versione più recente di ESET Endpoint Security. Se è disponibile una versione più recente, verrà segnalato all'utente durante il primo passaggio del processo di installazione. Se si seleziona l'opzione **Scarica e installa la nuova versione**, verrà scaricata la nuova versione e sarà possibile proseguire con l'installazione. Nel passaggio successivo verrà visualizzato l'Accordo di Licenza per l'Utente finale. Leggere e selezionare **Accetto** per confermare l'accettazione dei termini di tale Accordo. Dopo aver confermato l'accettazione, l'installazione procede seguendo due possibili scenari:

1. Se ESET Endpoint Security viene installato su un computer per la prima volta, verrà visualizzata la seguente finestra, dopo aver accettato l'**Accordo di Licenza per l'Utente Finale**. In questa finestra è possibile scegliere l'Installazione tipica o l'Installazione personalizzata e proseguire di conseguenza.


Installazione di ESET Endpoint Security
Modalità di installazione
Selezione della modalità di installazione
Scegliere se installare ESET Endpoint Security con le impostazioni tipiche (equilibrio ottimale tra protezione e velocità) o selezionare Personalizzata per accedere a opzioni di configurazione aggiuntive.
Modalità di installazione
Tipica (impostazioni migliori consigliate)
Personalizzata (configurazione più dettagliata)
< Indietro
Avanti >
Annulla

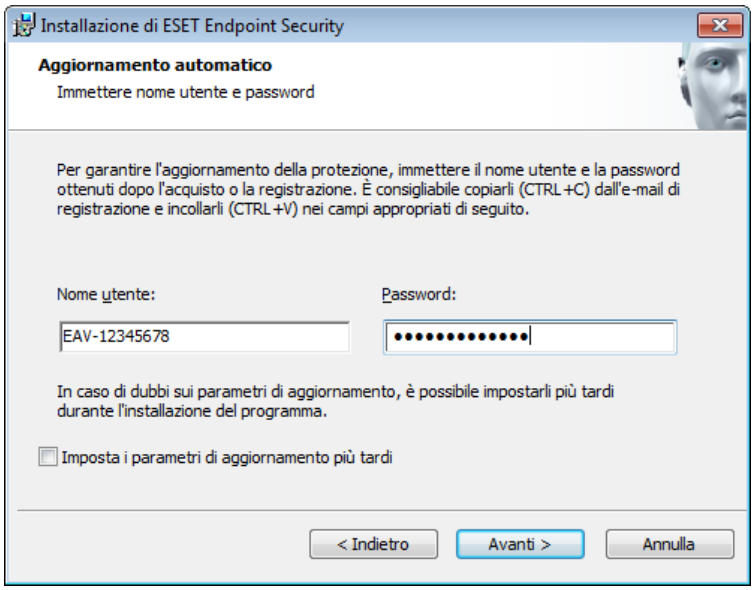
2. Se ESET Endpoint Security viene installato sopra una versione precedente del software, nella finestra seguente è possibile scegliere se utilizzare le impostazioni correnti del programma per la nuova installazione o, se l'opzione **Utilizza impostazioni correnti** è stata deselezionata, è possibile scegliere uno dei due metodi di installazione indicati in precedenza.


Installazione di ESET Endpoint Security
Modalità di installazione
Selezione della modalità di installazione
Se si desidera reinstallare il programma mantenendo le impostazioni correnti, non deselezionare questa casella di controllo.
Per reinstallare il programma e regolare le impostazioni, deselezionare la casella di controllo e selezionare una delle modalità di installazione.
Utilizza impostazioni correnti
Modalità di installazione
Tipica (impostazioni migliori consigliate)
Personalizzata (configurazione più dettagliata)
< Indietro
Avanti >
Annulla

2.1 Installazione tipica

La modalità di installazione tipica offre opzioni di configurazione adatte alla maggior parte degli utenti. Tali impostazioni assicurano protezione ottimale, facilità di utilizzo e prestazioni elevate del sistema. La modalità di installazione tipica rappresenta l'opzione predefinita consigliata nel caso in cui gli utenti non abbiano particolari necessità relative a impostazioni specifiche.

Dopo aver selezionato la modalità di installazione e aver selezionato **Avanti**, verrà chiesto di immettere il nome utente e la password per eseguire gli aggiornamenti automatici del programma. Ciò svolge un ruolo fondamentale per garantire una protezione costante del sistema.


Installazione di ESET Endpoint Security
Aggiornamento automatico
Immettere nome utente e password
Per garantire l'aggiornamento della protezione, immettere il nome utente e la password ottenuti dopo l'acquisto o la registrazione. È consigliabile copiarli (CTRL+C) dall'e-mail di registrazione e incollarli (CTRL+V) nei campi appropriati di seguito.
Nome utente:
Password:
EAV-12345678
In caso di dubbi sui parametri di aggiornamento, è possibile impostarli più tardi durante l'installazione del programma.
Imposta i parametri di aggiornamento più tardi
< Indietro
Avanti >
Annulla

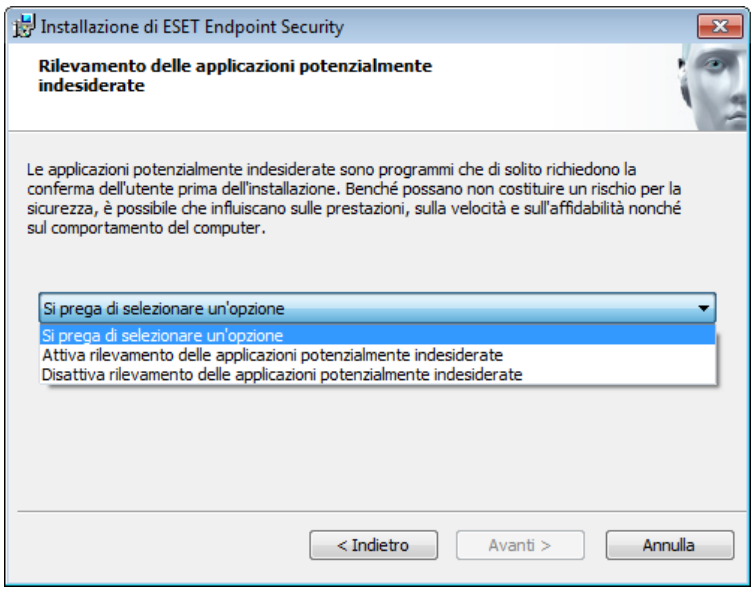
Immettere **Nome utente** e **Password** nei relativi campi, ovvero i dati di autenticazione ricevuti dopo aver acquistato o registrato il prodotto. Se al momento non si dispone di nome utente e password, fare clic sulla casella di controllo **Imposta i parametri di aggiornamento più tardi**. Il nome utente e la password possono essere immessi nel programma in seguito.

La fase successiva consiste nella configurazione di ESET Live Grid. ESET Live Grid consente di garantire che ESET sia informata in modo tempestivo e continuativo sulle nuove infiltrazioni così da proteggere gli utenti. Il sistema consente l'invio di nuove minacce ai laboratori antivirus ESET, dove i virus verranno analizzati, elaborati e aggiunti al database delle firme antivirali.

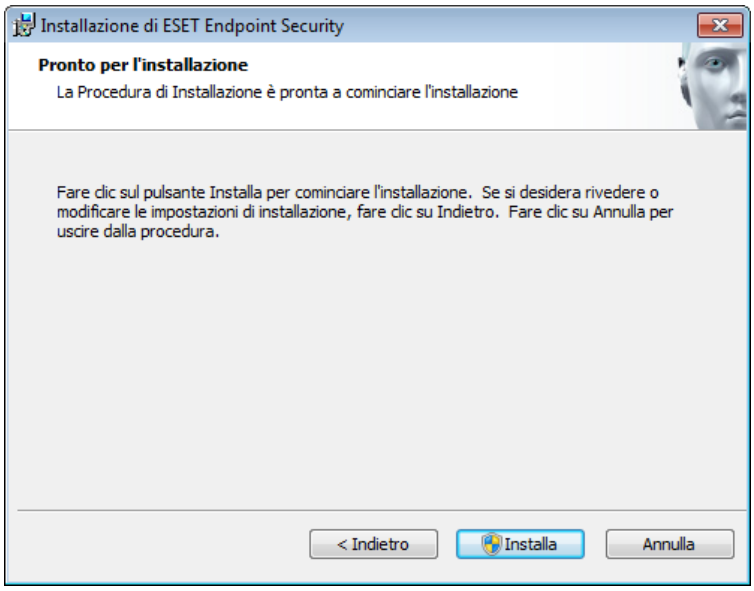
Installazione di ESET Endpoint Security
ESET Live Grid
Sviluppato sul sistema avanzato di allarme immediato ThreatSense.net, ESET Live Grid è progettato per offrire livelli aggiuntivi di protezione al computer. Controlla continuamente i programmi e i processi in esecuzione sul sistema rispetto alle informazioni più aggiornate raccolte tra milioni di utenti ESET in tutto il mondo. Le scansioni del sistema sono inoltre elaborate in maniera più rapida e precisa grazie all'ampliamento continuo del database ESET Live Grid.
Accetto di partecipare a ESET Live Grid (scelta consigliata)
< Indietro
Avanti >
Annulla

Per impostazione predefinita, l'opzione **Accetto di partecipare a ESET Live Grid** è selezionata e tale funzionalità sarà quindi attivata.

Il passaggio successivo del processo di installazione consiste nella configurazione dell'opzione di rilevamento delle applicazioni potenzialmente indesiderate. Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Per ulteriori informazioni, consultare il capitolo Applicazioni potenzialmente indesiderate.


Installazione di ESET Endpoint Security
Rilevamento delle applicazioni potenzialmente indesiderate
Le applicazioni potenzialmente indesiderate sono programmi che di solito richiedono la conferma dell'utente prima dell'installazione. Benché possano non costituire un rischio per la sicurezza, è possibile che influiscano sulle prestazioni, sulla velocità e sull'affidabilità nonché sul comportamento del computer.
Si prega di selezionare un'opzione
Si prega di selezionare un'opzione
Attiva rilevamento delle applicazioni potenzialmente indesiderate
Disattiva rilevamento delle applicazioni potenzialmente indesiderate
< Indietro
Avanti >
Annulla

L'ultimo passaggio della modalità di installazione tipica consiste nella conferma dell'installazione mediante il pulsante **Installa**.


Installazione di ESET Endpoint Security
Pronto per l'installazione
La Procedura di Installazione è pronta a cominciare l'installazione
Fare clic sul pulsante Installa per cominciare l'installazione. Se si desidera rivedere o modificare le impostazioni di installazione, fare clic su Indietro. Fare clic su Annulla per uscire dalla procedura.
< Indietro
Installa
Annulla

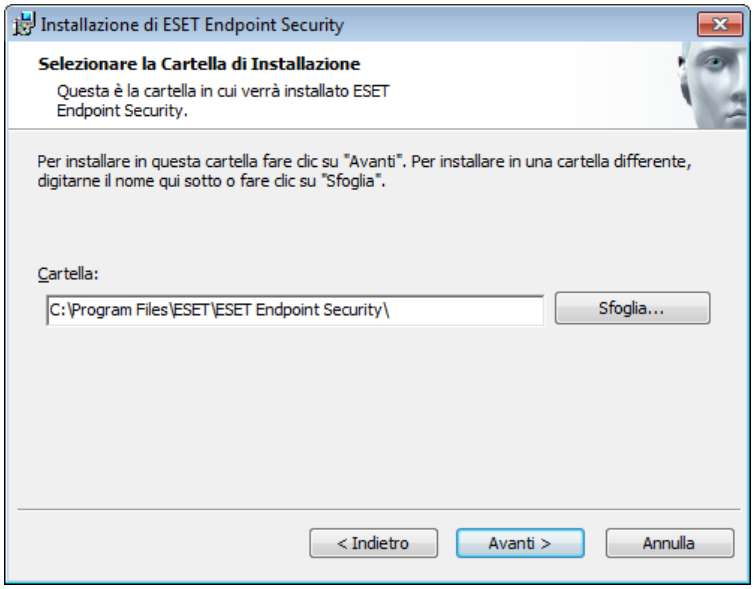
2.2 Installazione personalizzata

La modalità di installazione personalizzata è indicata per utenti con esperienza nella configurazione dettagliata dei programmi e che desiderano modificare le impostazioni avanzate durante l'installazione.

Dopo aver selezionato questa modalità di installazione e aver selezionato **Avanti**, verrà chiesto di selezionare un percorso di destinazione per l'installazione. Per impostazione predefinita, il programma viene installato nella directory seguente:

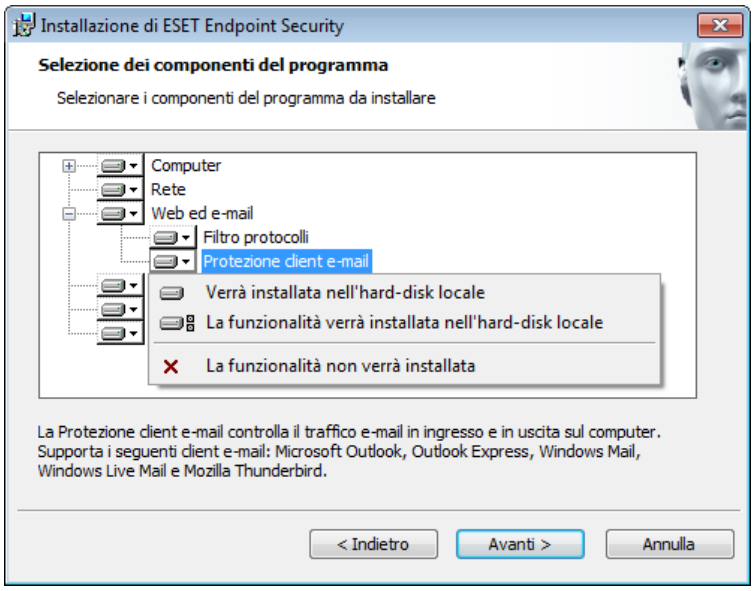
C:\Programmi\ESET\ESET Endpoint Security\

Scegliere **Sfoglia...** per selezionare un percorso diverso (scelta non consigliata).

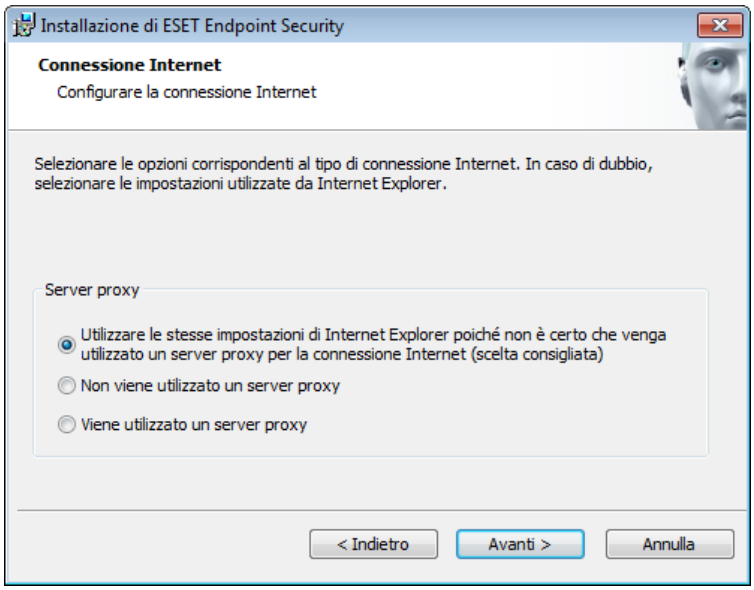

Installazione di ESET Endpoint Security
Selezionare la Cartella di Installazione
Questa è la cartella in cui verrà installato ESET Endpoint Security.
Per installare in questa cartella fare clic su "Avanti". Per installare in una cartella differente, digitarne il nome qui sotto o fare clic su "Sfoglia".
Cartella:
C:\Program Files\ESET\ESET Endpoint Security\
Sfoglia...
< Indietro
Avanti >
Annulla

Quindi, immettere il **Nome utente** e **Password**. Questo passaggio è analogo a quello dell'Installazione tipica (consultare "Installazione tipica").

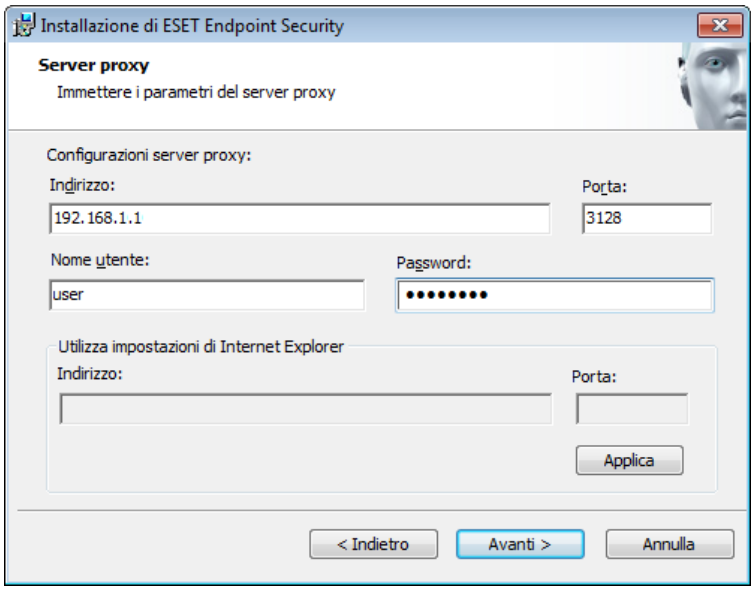
Il passaggio successivo del processo di installazione consiste nella scelta dei componenti di programma da installare. Espandere la struttura dei componenti e selezionare una funzionalità per visualizzare le tre opzioni di installazione. Per impostazione predefinita è selezionata l'opzione **Verrà installata nell'hard disk locale**. Selezionare **La funzionalità verrà installata nell'hard-disk locale** per installare tutte le funzionalità nella struttura selezionata. Se non si desidera utilizzare una funzionalità o un componente, selezionare **La funzionalità non verrà installata**.


Installazione di ESET Endpoint Security
Selezione dei componenti del programma
Selezionare i componenti del programma da installare
Computer
Rete
Web ed e-mail
Filtro protocolli
Protezione client e-mail
Verrà installata nell'hard-disk locale
La funzionalità verrà installata nell'hard-disk locale
La funzionalità non verrà installata
La Protezione client e-mail controlla il traffico e-mail in ingresso e in uscita sul computer. Supporta i seguenti client e-mail: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.
< Indietro
Avanti >
Annulla

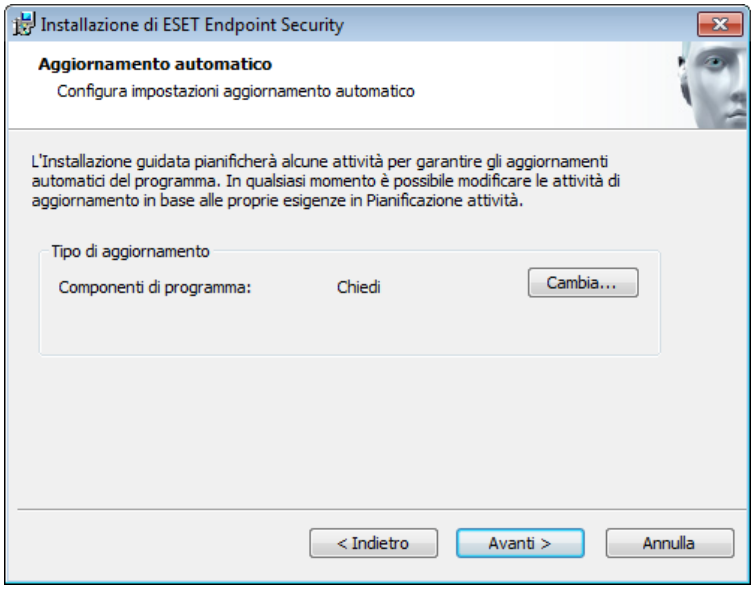
Fare clic su **Avanti** per passare alla configurazione Internet. Se si utilizza un server proxy, è necessario configurarlo correttamente per l'esecuzione degli aggiornamenti delle firme antivirali. Se non si è certi che venga utilizzato un server proxy per connettersi a Internet, selezionare l'opzione **Utilizzare le stesse impostazioni di Internet Explorer poiché non è certo che venga utilizzato un server proxy per la connessione Internet (scelta consigliata)**, quindi fare clic su **Avanti**. Se non si utilizza un server proxy, selezionare l'opzione **Non viene utilizzato un server proxy**.


Installazione di ESET Endpoint Security
Connessione Internet
Configurare la connessione Internet
Selezionare le opzioni corrispondenti al tipo di connessione Internet. In caso di dubbio, selezionare le impostazioni utilizzate da Internet Explorer.
Server proxy
Utilizzare le stesse impostazioni di Internet Explorer poiché non è certo che venga utilizzato un server proxy per la connessione Internet (scelta consigliata)
Non viene utilizzato un server proxy
Viene utilizzato un server proxy
< Indietro
Avanti >
Annulla

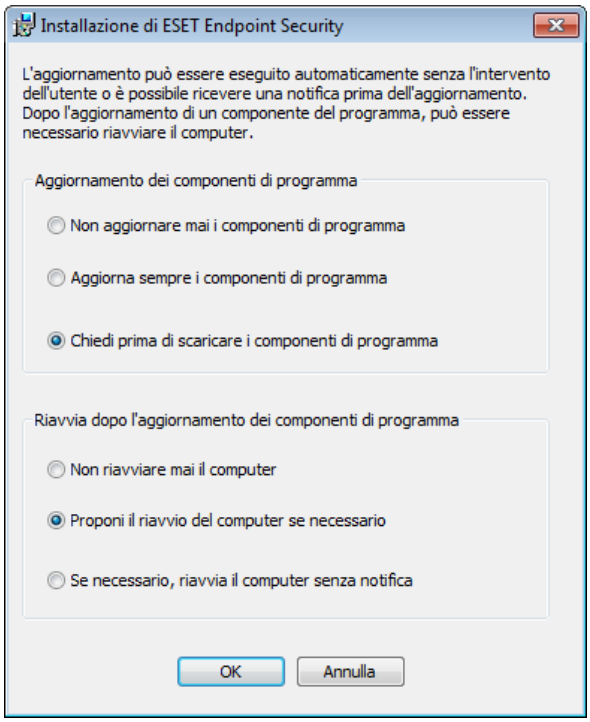
Per configurare le impostazioni del server proxy, selezionare **Viene utilizzato un server proxy**, quindi fare clic su **Avanti**. Immettere l'indirizzo IP o l'URL del server proxy nel campo **Indirizzo**. Nel campo **Porta** specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Nel caso in cui il server proxy richieda l'autenticazione, sarà necessario immettere un **Nome utente** e **Password** validi per consentire l'accesso al server proxy. Se si desidera è anche possibile copiare le impostazioni del server proxy da Internet Explorer.. A tale scopo, fare clic su **Applica** e confermare la selezione.



In questa fase dell'installazione è possibile specificare la modalità di gestione degli aggiornamenti automatici del programma sul sistema. Scegliere **Cambia...** per accedere alle impostazioni avanzate.

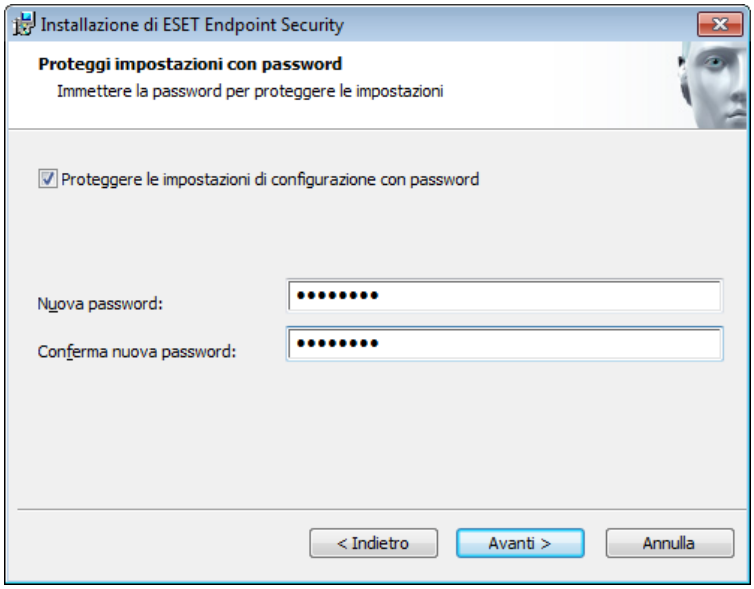

Installazione di ESET Endpoint Security
Aggiornamento automatico
Configura impostazioni aggiornamento automatico
L'Installazione guidata pianificherà alcune attività per garantire gli aggiornamenti automatici del programma. In qualsiasi momento è possibile modificare le attività di aggiornamento in base alle proprie esigenze in Pianificazione attività.
Tipo di aggiornamento
Componenti di programma:
Chiedi
Cambia...
< Indietro
Avanti >
Annulla

Se non si desidera aggiornare i componenti di programma, selezionare l'opzione **Non aggiornare mai i componenti di programma**. Selezionare l'opzione **Chiedi prima di scaricare i componenti di programma** per visualizzare una finestra di conferma ogni volta che il sistema tenta di scaricare i componenti di programma. Per scaricare automaticamente gli aggiornamenti dei componenti di programma, selezionare l'opzione **Aggiorna sempre i componenti di programma**.


Installazione di ESET Endpoint Security
L'aggiornamento può essere eseguito automaticamente senza l'intervento dell'utente o è possibile ricevere una notifica prima dell'aggiornamento. Dopo l'aggiornamento di un componente del programma, può essere necessario riavviare il computer.
Aggiornamento dei componenti di programma
Non aggiornare mai i componenti di programma
Aggiorna sempre i componenti di programma
Chiedi prima di scaricare i componenti di programma
Riavvia dopo l'aggiornamento dei componenti di programma
Non riavviare mai il computer
Proponi il riavvio del computer se necessario
Se necessario, riavvia il computer senza notifica
OK
Annulla

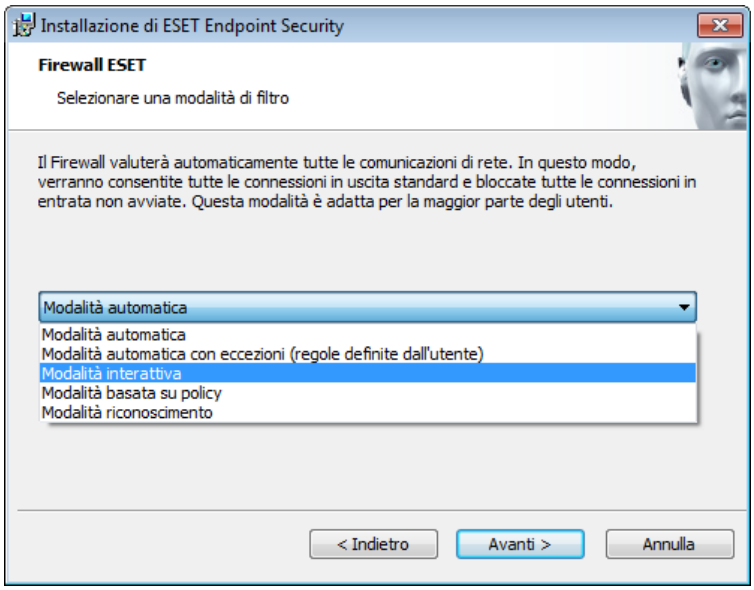
NOTA: in genere, dopo aver aggiornato un componente di programma, è necessario riavviare il sistema. Si consiglia di selezionare l'opzione **Se necessario, riavvia il computer senza notifica**.

Nella finestra di installazione successiva è disponibile l'opzione per impostare una password per proteggere le impostazioni del programma. Selezionare l'opzione **Proteggere le impostazioni di configurazione con password** e immettere la password nei campi **Nuova password** e **Conferma nuova password**. La password verrà richiesta per modificare o accedere alle impostazioni di ESET Endpoint Security. Se i campi delle password corrispondono, fare clic su **Avanti** per continuare.


Installazione di ESET Endpoint Security
Proteggi impostazioni con password
Immettere la password per proteggere le impostazioni
Proteggere le impostazioni di configurazione con password
Nuova password:
Conferma nuova password:
< Indietro
Avanti >
Annulla

I successivi passaggi dell'installazione, **Aggiornamento automatico**, **ESET Live Grid** e **Rilevamento di applicazioni potenzialmente indesiderate** sono uguali alla modalità Installazione tipica (consultare "Installazione tipica").

Quindi, selezionare la modalità di filtro del Firewall ESET. Per il Firewall ESET Endpoint Security sono disponibili cinque modalità di filtraggio. Il comportamento del firewall varia in base alla modalità selezionata. Le Modalità di filtro influenzano inoltre il livello di interazione da parte dell'utente.


Installazione di ESET Endpoint Security
Firewall ESET
Selezionare una modalità di filtro
Il Firewall valuterà automaticamente tutte le comunicazioni di rete. In questo modo, verranno consentite tutte le connessioni in uscita standard e bloccate tutte le connessioni in entrata non avviate. Questa modalità è adatta per la maggior parte degli utenti.
Modalità automatica
Modalità automatica
Modalità automatica con eccezioni (regole definite dall'utente)
Modalità interattiva
Modalità basata su policy
Modalità riconoscimento
< Indietro
Avanti >
Annulla

Fare clic su **Installa** nella finestra **Pronto all'installazione** per completare l'installazione. Al termine dell'installazione, all'utente verrà richiesto di attivare il prodotto. Per ulteriori informazioni sull'attivazione del prodotto, consultare Installazione tipica.

2.3 Inserimento di nome utente e password

Per garantire una funzionalità ottimale è fondamentale che il programma venga aggiornato automaticamente. Ciò è possibile solo se il nome utente e la password vengono immessi correttamente nell'**Impostazione aggiornamento**.

Nel caso in cui nome utente e password non siano stati immessi durante l'installazione, è possibile inserirli ora. Premere **CTRL+U** e inserire i dati della licenza ricevuti insieme al prodotto di protezione ESET nella finestra Dettagli licenza.

Quando si immette il **Nome utente** e **Password**, è importante immetterli esattamente come sono scritti:

- Il nome utente e la password fanno distinzione tra maiuscole e minuscole e nel nome utente è necessaria la lineetta.
- La password è composta da dieci caratteri scritti tutti in lettere minuscole.
- La lettera L non viene utilizzata nelle password (al suo posto viene usato il numero uno (1)).
- Un grande "O" corrisponde al numero zero (0), mentre una piccola "o" corrisponde alla lettera o scritta in minuscolo.

Per evitare errori, si consiglia di copiare e incollare i dati dal messaggio e-mail di registrazione.

2.4 Aggiornamento ad una versione più recente

Versioni più recenti di ESET Endpoint Security vengono rilasciate per apportare miglioramenti o correggere problemi che non è possibile risolvere mediante l'aggiornamento automatico dei moduli del programma. L'aggiornamento a una versione più recente può essere eseguito in diversi modi:

1. Automaticamente tramite un aggiornamento del programma.
   Poiché l'aggiornamento del programma viene distribuito a tutti gli utenti e può influenzare alcune configurazioni del sistema, viene rilasciato per un lungo periodo di prova per consentirne l'utilizzo su tutte le possibili configurazioni di sistema. Se è necessario eseguire l'aggiornamento a una versione più recente nel momento in cui viene rilasciato, usare uno dei metodi seguenti.
2. Manualmente scaricando e installando una versione più recente su quella precedente.
   All'inizio dell'installazione, è possibile scegliere di preservare le impostazioni correnti del programma selezionando la casella di controllo **Utilizza impostazioni correnti**.
3. Manualmente tramite la distribuzione automatica in un ambiente di rete tramite ESET Remote Administrator.

2.5 Controllo computer

Dopo aver installato ESET Endpoint Security, è necessario eseguire un controllo del computer alla ricerca di codici dannosi. Nella finestra principale del programma, fare clic su **Controllo computer**, quindi selezionare **Controllo intelligente**. Per ulteriori informazioni sui controlli del computer, consultare la sezione Controllo computer.

3. Guida introduttiva

In questo capitolo viene fornita una panoramica su ESET Endpoint Security e sulle configurazioni di base.

3.1 Introduzione all'interfaccia utente

La finestra principale di ESET Endpoint Security è suddivisa in due sezioni principali. La finestra principale sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Di seguito è riportata una descrizione delle opzioni del menu principale:

Stato protezione - Fornisce informazioni relative allo stato di protezione di ESET Endpoint Security.

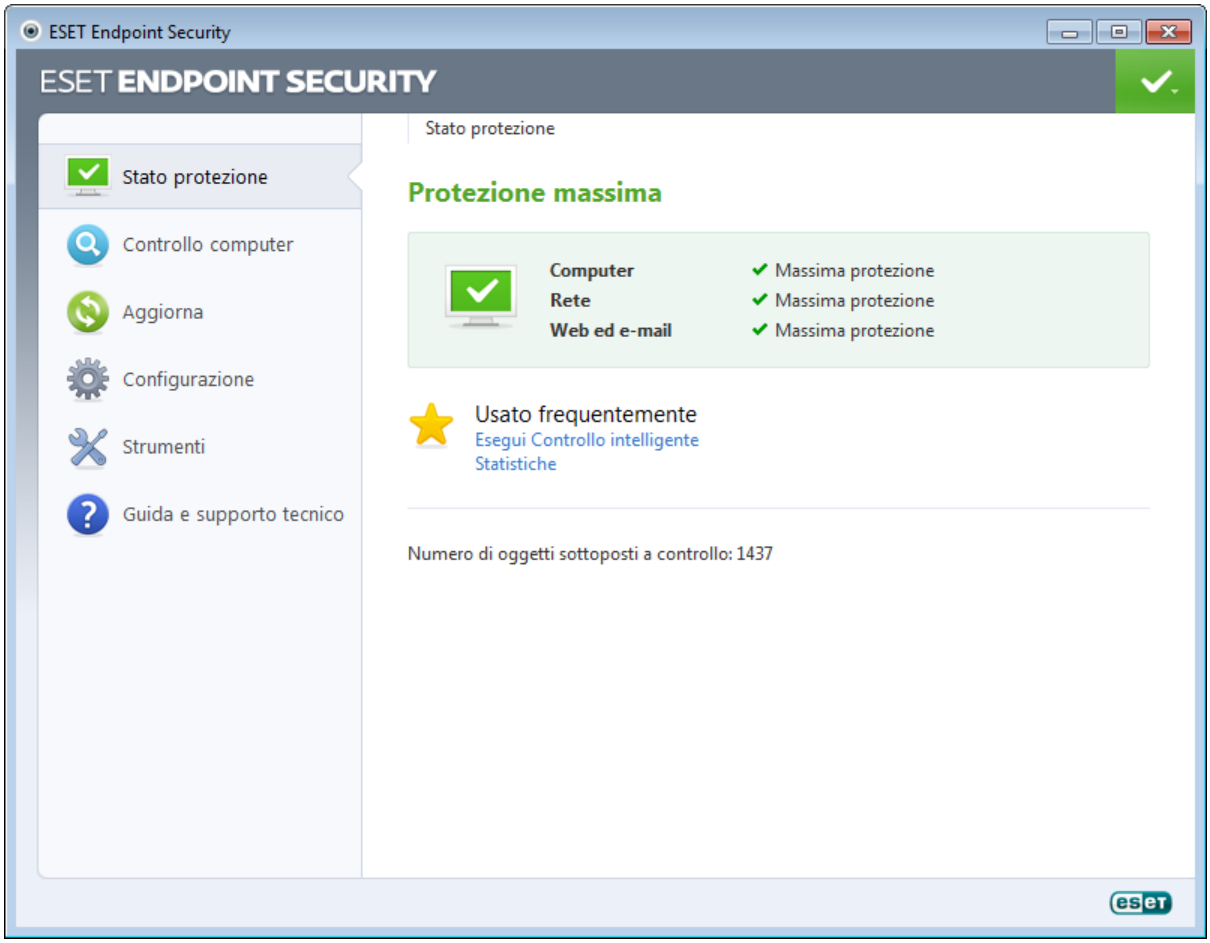
Controllo computer - Questa opzione consente di configurare e avviare un Controllo intelligente o un Controllo personalizzato.

Aggiorna - Consente di visualizzare informazioni relative agli aggiornamenti del database delle firme antivirali.

Configurazione - Selezionare questa opzione per regolare il livello di protezione per Computer, Web ed e-mail. e Rete .

Strumenti - Consente di accedere ai File di rapporto, Statistiche di protezione, Attività di verifica, Processi in esecuzione, Connessioni di rete, Pianificazione attività, Quarantena, ESET SysInspector e ESET SysRescue.

Guida e supporto tecnico - Consente di accedere ai file della Guida, alla Knowledge Base ESET, al sito Web ESET e ai collegamenti per aprire una richiesta di assistenza al Supporto tecnico.



Nella schermata **Stato protezione** sono visualizzate informazioni sulla sicurezza e sul livello di protezione corrente del computer. Lo stato **Protezione massima** verde indica che è garantito il livello massimo di protezione.

Nella finestra di stato sono inoltre visualizzate le funzionalità di ESET Endpoint Security usate più frequentemente. In questa finestra sono inoltre disponibili informazioni sulla data di scadenza del programma.

3.2 Cosa fare se il programma non funziona correttamente

Se i moduli attivati funzionano correttamente, verrà visualizzato un segno di spunta di controllo verde. In caso contrario, verrà visualizzato un punto esclamativo rosso o un'icona di notifica arancione. Nella parte superiore della finestra, verranno visualizzate ulteriori informazioni sul modulo. Verrà inoltre visualizzata una soluzione consigliata per la riparazione del modulo. Per modificare lo stato dei singoli moduli, scegliere **Configurazione** dal menu principale e fare clic sul modulo desiderato.

ESET Endpoint Security
ESET ENDPOINT SECURITY
Stato protezione
Controllo computer
Aggiorna
Configurazione
Strumenti
Guida e supporto tecnico
Stato protezione
La protezione massima non è garantita
Computer
Rete
Web ed e-mail
Rischio per la protezione
Massima protezione
Rischio per la protezione
Protezione antivirus disattivata
Alcuni moduli della protezione antivirus e antispyware sono stati disattivati dall'utente. È possibile attivare la protezione completa qui: Avvia tutti i moduli della protezione antivirus e antispyware
Il sistema operativo non è aggiornato
Nel computer non sono installati tutti gli aggiornamenti disponibili del sistema operativo. Installare gli aggiornamenti mancanti tramite il servizio Windows Update. Per ulteriori informazioni, fare clic qui.
Usato frequentemente
Esegui Controllo intelligente
Statistiche
Numero di oggetti sottoposti a controllo: 3591
Licenza valida fino al: 29. 12. 2012
eset

Le segnalazioni con icone di colore rosso indicano che sono presenti problemi critici, ovvero che non è garantito il livello massimo di protezione. Le cause possibili sono:

- Protezione file system in tempo reale disattivata
- Firewall disattivato
- Database delle firme antivirali non aggiornato
- Prodotto non attivato
- Licenza del prodotto scaduta

L'icona di colore arancione indica che l'accesso Web o la protezione client di posta è disattivata, si è verificato un problema durante l'aggiornamento del programma (database delle firme antivirali non aggiornato e impossibilità di eseguire l'aggiornamento) o la licenza sta per scadere.

Protezione antivirus e antispyware disattivata - Questo problema è segnalato da un'icona rossa e da una notifica di protezione accanto alla voce **Computer**. È possibile riattivare la protezione antivirus e antispyware facendo clic su **Avvia tutti i moduli di protezione antivirus e antispyware**.

Protezione accesso Web disattivata - Questo problema è segnalato da un'icona arancione con una "i" e dallo stato **Notifica di protezione**. È possibile riattivare la Protezione accesso Web facendo clic sulla notifica di protezione e selezionando **Attiva protezione accesso Web**.

Firewall ESET disattivato - Questo problema è segnalato da un'icona rossa e da una notifica di protezione accanto alla voce **Rete**. È possibile riattivare la protezione della rete facendo clic su **Attiva modalità di filtro**.

La licenza scadrà a breve - Questa condizione è indicata dalla presenza di un'icona dello stato di protezione contenente un punto esclamativo. Allo scadere della licenza, non sarà possibile aggiornare il programma e l'icona dello stato di protezione diventerà rossa.

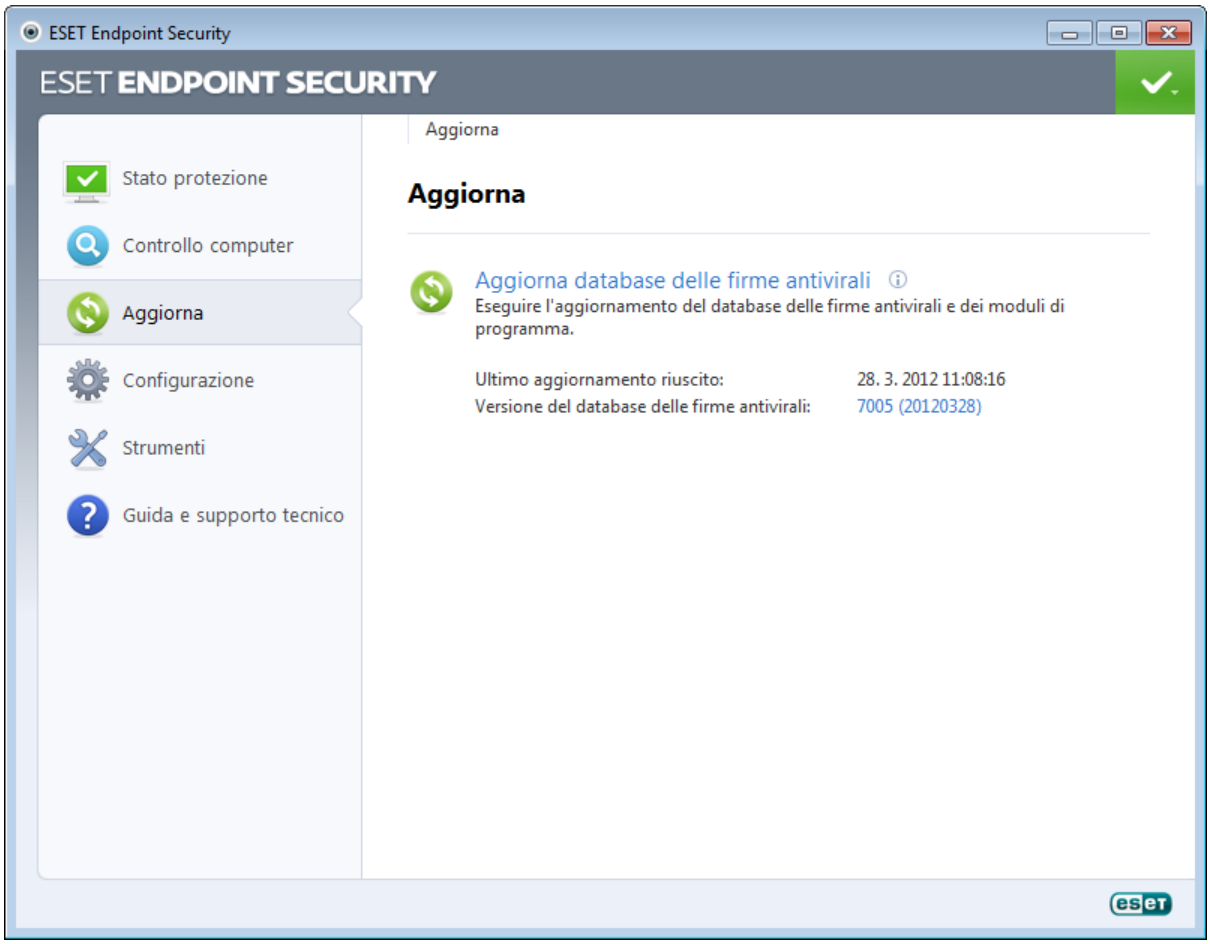
Licenza scaduta - Questa condizione è indicata dalla presenza di un'icona rossa dello stato di protezione. Allo scadere della licenza, non sarà possibile aggiornare il programma. Si consiglia di seguire le istruzioni nella finestra di avviso per rinnovare la licenza.

Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, fare clic su **Guida e supporto tecnico** per accedere ai file della Guida o effettuare una ricerca nella Knowledge Base ESET. Nel caso in cui sia necessaria assistenza è possibile inviare una richiesta al Supporto tecnico ESET. Il Supporto tecnico ESET risponderà rapidamente alle domande degli utenti e li aiuterà a trovare una soluzione ai loro problemi.

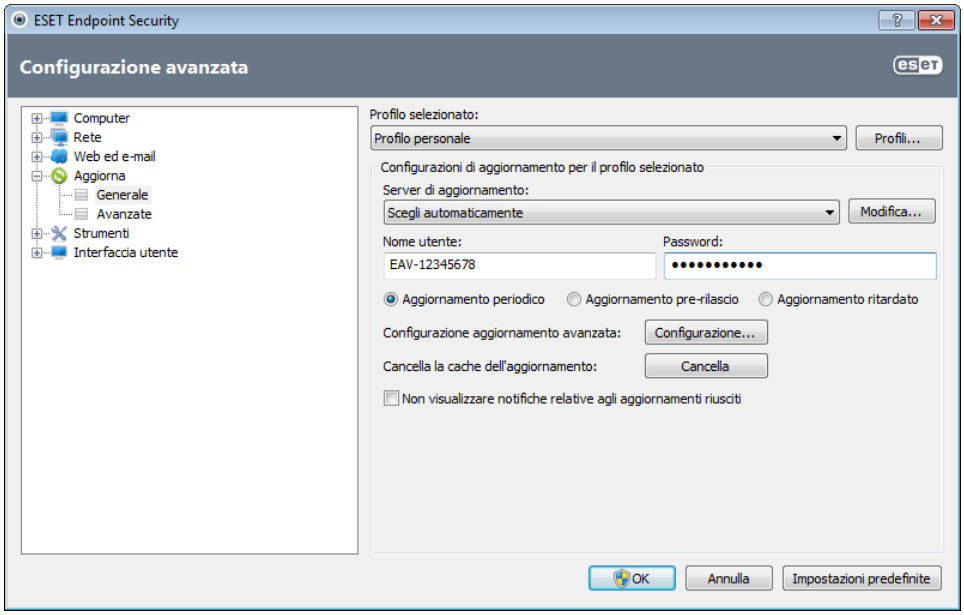
3.3 Configurazione dell'aggiornamento

L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi. È opportuno prestare attenzione alla relativa configurazione e al funzionamento. Nel menu principale, selezionare **Aggiorna**, quindi fare clic su **Aggiorna database delle firme antivirali** per verificare la disponibilità di un aggiornamento recente del database.

Nel caso in cui nome utente e password non siano stati immessi durante il processo di e installazione di ESET Endpoint Security, verrà richiesto di immetterli ora.

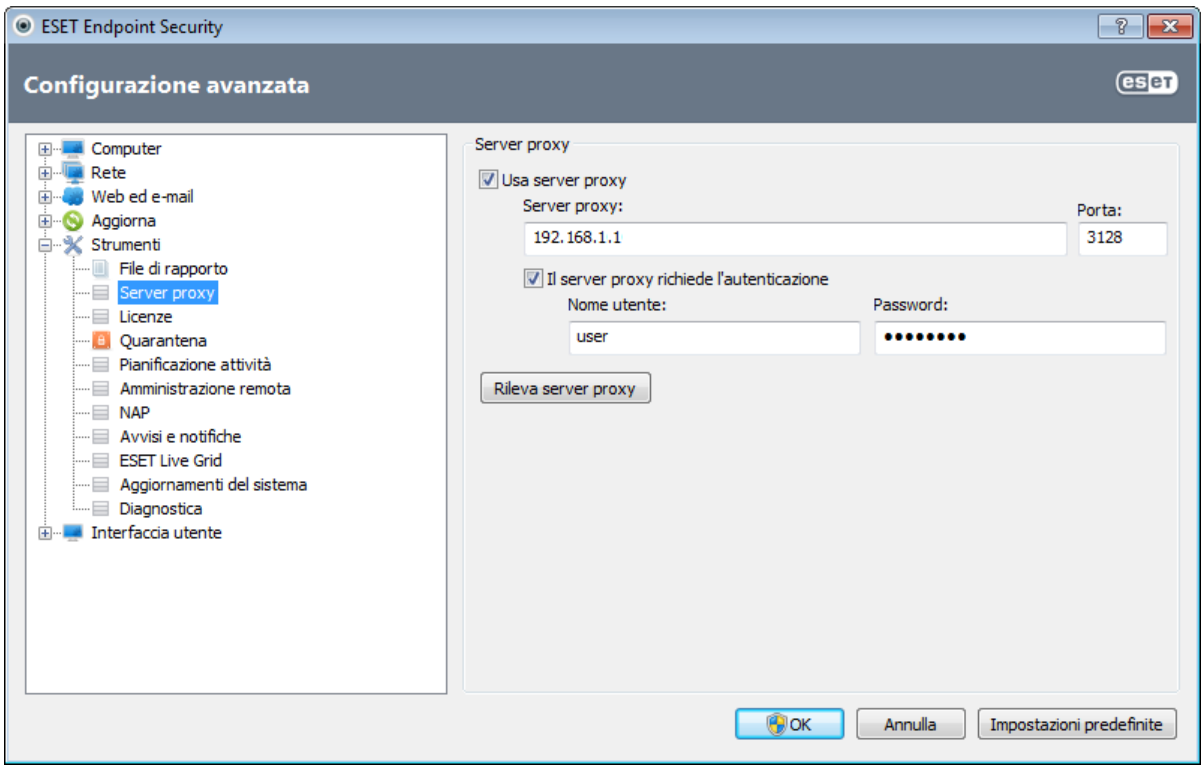


Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi selezionare **Accedi a configurazione avanzata...** oppure premere F5 sulla tastiera) sono disponibili ulteriori opzioni di aggiornamento. Fare clic su **Aggiorna** nella struttura Configurazione avanzata a sinistra. Per impostazione predefinita, il menu a discesa **Server di aggiornamento** è impostato su **Scegli automaticamente**. Per configurare le opzioni di aggiornamento avanzate, ad esempio la modalità di aggiornamento, l'accesso al server proxy, le connessioni LAN e la creazione di copie delle firme antivirali, fare clic sul pulsante **Configurazione...**.



3.4 Configurazione del server proxy

Nel caso in cui si utilizzi un server proxy per controllare le connessioni a Internet su un sistema che utilizza ESET Endpoint Security, deve essere specificato nella finestra Configurazione avanzata. Per accedere alla finestra di configurazione del server proxy, premere F5 per aprire la finestra Configurazione avanzata e fare clic su **Strumenti** > **Server proxy** nella struttura Configurazione avanzata. Selezionare l'opzione **Utilizza server proxy**, quindi compilare i campi **Server proxy** (indirizzo IP) e **Porta**. Se necessario, selezionare l'opzione **Il server proxy richiede l'autenticazione**, quindi immettere **Nome utente** e **Password**.

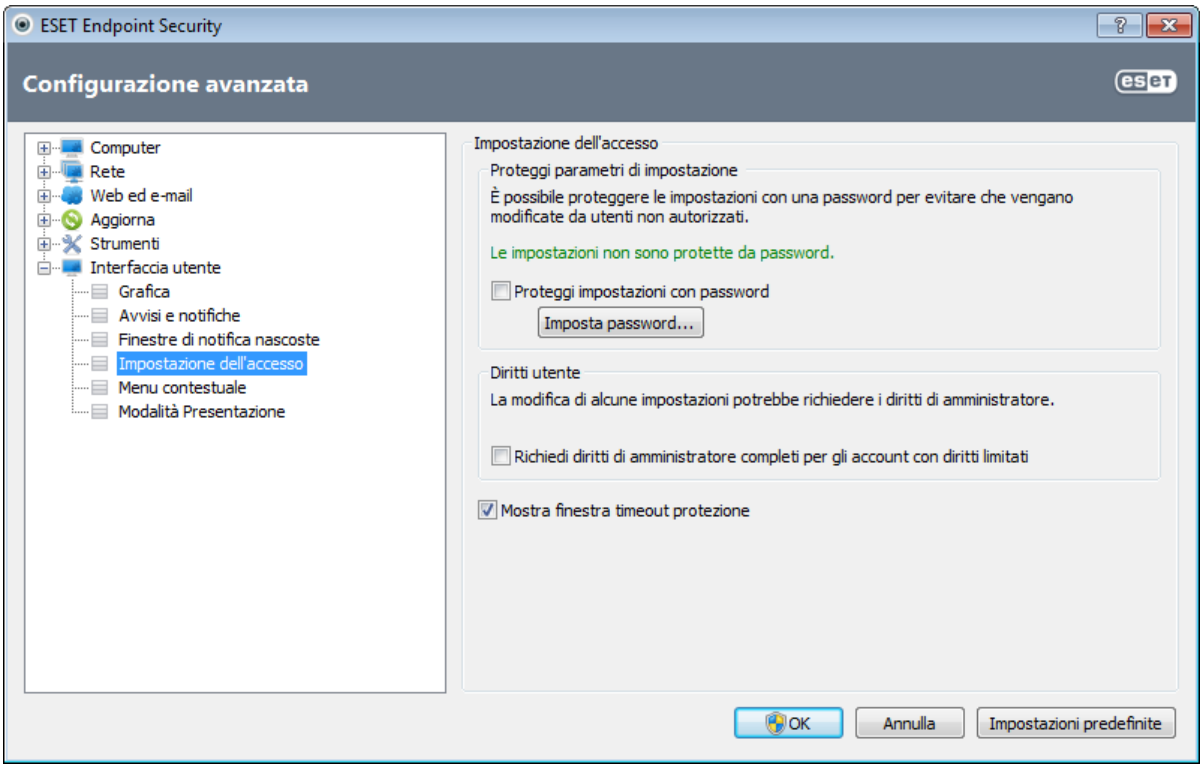


Se queste informazioni non sono disponibili, provare a rilevare automaticamente le impostazioni del server proxy facendo clic sul pulsante **Rileva server proxy**.

NOTA: le opzioni del server proxy potrebbero essere diverse in base ai diversi profili di aggiornamento. In questo caso, configurare i diversi profili di aggiornamento nella finestra Configurazione avanzata facendo clic su **Aggiorna** nella struttura Configurazione avanzata.

3.5 Impostazione protezione

Le impostazioni di ESET Endpoint Security rivestono un ruolo fondamentale dal punto di vista dei criteri di protezione. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Per proteggere con password i parametri di configurazione, nel menu principale fare clic su **Configurazione** > **Accedi a configurazione avanzata...** > **Interfaccia utente** > **Impostazione dell'accesso**, selezionare l'opzione **Proteggi impostazioni con password** e fare clic sul pulsante **Imposta password...**.



Immettere una nuova password nei campi **Nuova password** e **Conferma nuova password**, quindi fare clic su **OK**. La password verrà richiesta per apportare future modifiche alle impostazioni di ESET Endpoint Security.

3.6 Configurazione area sicura

È necessario configurare l'area affidabile per proteggere il computer in un ambiente di rete. Attraverso la configurazione dell'area affidabile per consentire la condivisione, è possibile consentire l'accesso al computer da parte di altri utenti. Fare clic su **Configurazione** > **Rete** > **Modifica la modalità di protezione del computer nella rete...**. Verrà visualizzata una finestra contenente opzioni che consentono di scegliere la modalità di protezione desiderata per il computer nella rete.

Il rilevamento dell'area affidabile viene eseguito dopo l'installazione di ESET Endpoint Security e ogni volta che il computer si connette a una nuova rete. In molti casi non è pertanto necessario definire l'Area affidabile. Per impostazione predefinita, al rilevamento di una nuova area verrà visualizzata una finestra di dialogo che consente di impostare il livello di protezione per quell'area.

ESET Endpoint Security
Rilevata nuova connessione di rete
Scegliere la modalità di protezione del computer nella rete:
Subnet: 10.0.2.0 / 255.255.255.0
Suffisso DNSx: hq.eset.com
Indirizzi DHCP: 10.0.2.2
Massima protezione - Rete pubblica
Il computer non sarà visibile ad altri computer nella rete (ad esempio le cartelle o le stampanti condivise non saranno visibili da altri computer nella rete). Un esempio di questo tipo di connessione è una rete pubblica.
Consenti condivisione - Rete domestica
Il computer sarà visibile ad altri computer nella rete (ad esempio le cartelle o le stampanti condivise saranno visibili da altri computer nella rete). Un esempio di questo tipo di connessione è una rete pubblica.
La modalità selezionata può essere cambiata in un secondo momento nella sezione Configurazione
Configurazione avanzata...
Annulla

Attenzione: una configurazione dell'area affidabile non corretta potrebbe costituire un rischio per la protezione del computer.

NOTA: per impostazione predefinita, le workstation di un'area attendibile possono accedere a file e stampanti condivisi; è attivata, inoltre, la comunicazione RPC in entrata ed è disponibile la condivisione del desktop remoto.

4. Utilizzo di ESET Endpoint Security

Le opzioni di impostazione di ESET Endpoint Security consentono di configurare i livelli di protezione della rete e del computer in uso.

Il menu **Configurazione** contiene le opzioni seguenti:

- **Computer**
- **Rete**
- **Web ed e-mail**

Fare clic su un componente per regolare le impostazioni avanzate del modulo di protezione corrispondente.

L'impostazione della protezione **Computer** consente di attivare o disattivare i componenti seguenti:

- **Protezione file system in tempo reale** - Tutti i file vengono sottoposti a controllo per la ricerca di codici dannosi al momento dell'apertura, creazione o esecuzione sul computer.
- **Protezione documenti** - La funzione Protezione documenti consente di eseguire il controllo dei documenti di Microsoft Office prima della loro apertura e dei file scaricati automaticamente da Internet Explorer, ad esempio gli elementi di Microsoft ActiveX.
- **Controllo dispositivi** - Questo modulo consente di controllare, bloccare o regolare i filtri/autorizzazioni e scegliere le modalità di accesso e di utilizzo di un determinato supporto da parte dell'utente (CD/DVD/USB, ecc.).
- **HIPS** - Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a una serie personalizzata di regole.
- **Modalità Presentazione** - Attiva o disattiva la Modalità Presentazione. Viene visualizzato un messaggio di avviso (potenziale rischio per la protezione) e la finestra principale diventa arancione quando si attiva la Modalità Presentazione.
- **Protezione Anti-Stealth** - Consente di rilevare i programmi pericolosi, ad esempio rootkit, che riescono a nascondersi dal sistema operativo. Ciò significa che non è possibile rilevarli utilizzando le normali tecnologie di testing.

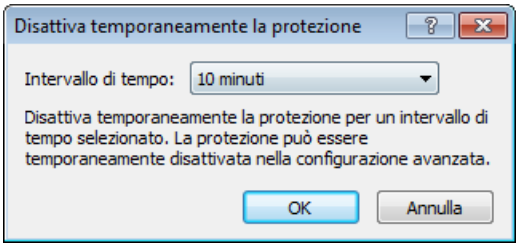
La sezione **Rete** consente di attivare o disattivare il **Firewall personale**.

L'impostazione della protezione **Web ed e-mail** consente di attivare o disattivare i componenti seguenti:

- **Protezione accesso Web** - Se questa opzione è attivata, viene eseguito il controllo di tutto il traffico HTTP o HTTPS per rilevare software dannoso.
- **Protezione client e-mail** - Monitora le comunicazioni ricevute mediante il protocollo POP3 e IMAP.
- **Protezione antispam** - Controlla i messaggi e-mail non desiderati, ad esempio lo spamming.
- **Controllo Web** - Consente di bloccare le pagine Web che possono contenere materiale potenzialmente inappropriato. I datori di lavoro o amministratori di sistema possono inoltre vietare l'accesso fino a 27 categorie di siti Web predefinite.

NOTA: la Protezione documenti è disponibile dopo aver attivato l'opzione (**Accedi a configurazione avanzata...** (F5) > **Computer** > **Antivirus e antispyware** > **Protezione documenti** > **Integrazione nel sistema**).

Dopo aver selezionato **Attivato**, viene visualizzata la finestra di dialogo **Disattiva temporaneamente la protezione**. Fare clic su **OK** per disattivare il componente di protezione selezionato. Nel menu a discesa **Intervallo di tempo** viene visualizzato il periodo di tempo in cui il componente selezionato sarà disattivato.


Disattiva temporaneamente la protezione
Intervallo di tempo:
10 minuti
Disattiva temporaneamente la protezione per un intervallo di tempo selezionato. La protezione può essere temporaneamente disattivata nella configurazione avanzata.
OK
Annulla

Per attivare nuovamente la protezione del componente di protezione disattivato, fare clic su **Disattivato**.

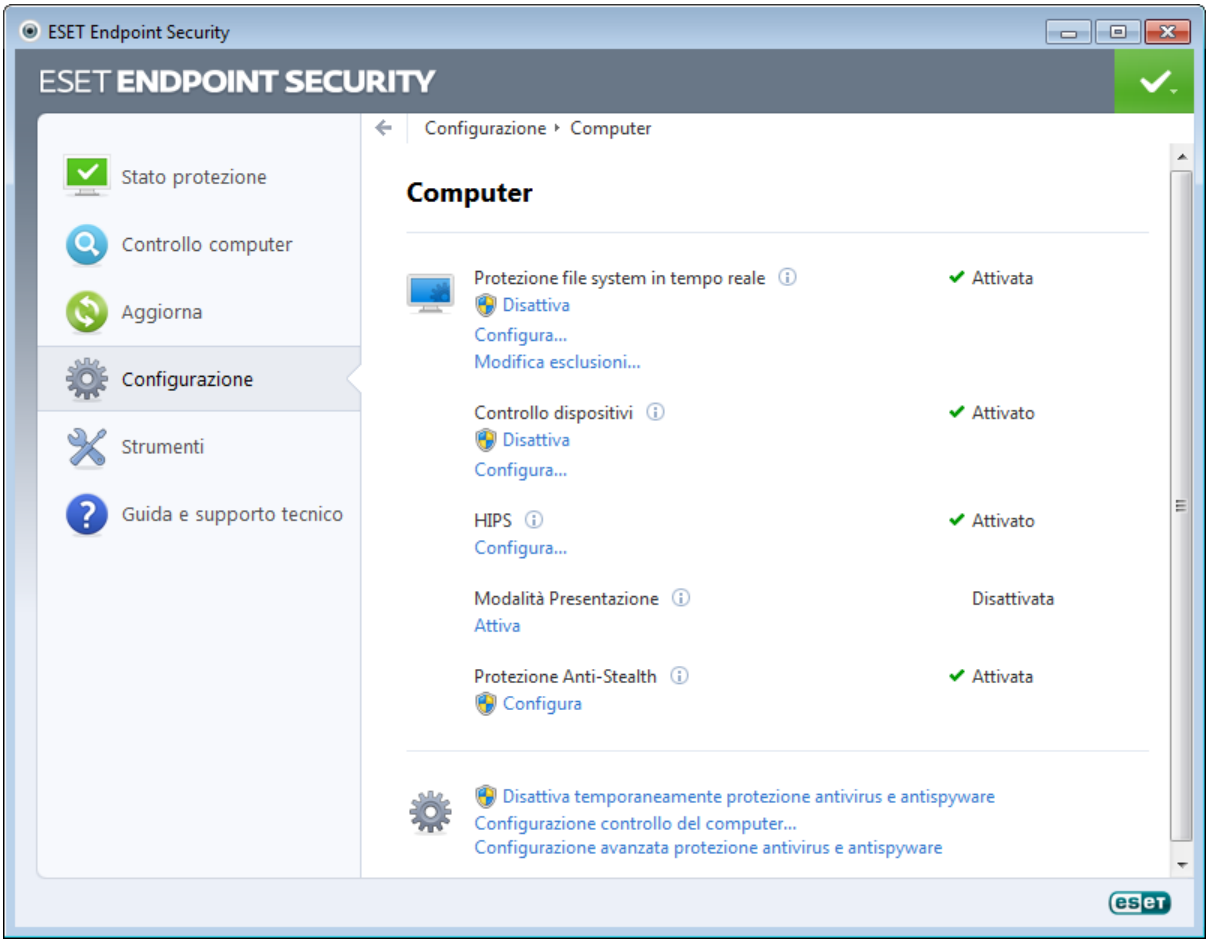
NOTA: quando si disattiva la protezione mediante questo metodo, tutte le parti disattivate della protezione saranno attivate dopo aver riavviato il computer.

Nella parte inferiore della finestra di configurazione sono disponibili ulteriori opzioni. Per caricare i parametri di impostazione mediante un file di configurazione .xml o per salvare i parametri di impostazione correnti su un file di configurazione, selezionare l'opzione **Importa ed esporta impostazioni...**.

4.1 Computer

Il modulo **Computer** è disponibile nel riquadro **Configurazione** facendo clic sul titolo **Computer**. Questa finestra mostra una panoramica di tutti i moduli di protezione. Per disattivare temporaneamente i singoli moduli, fare clic su **Disattiva** sotto il modulo desiderato. Tenere presente che in questo modo si potrebbe ridurre la protezione del computer. Per accedere alle impostazioni dettagliate di ciascun modulo, fare clic su **Configura...**.

Fare clic su **Modifica esclusioni...** per aprire la finestra di configurazione Esclusione, che consente di escludere i file e le cartelle dal controllo.



Disattiva temporaneamente la protezione antivirus e antispyware - Disattiva tutti i moduli di protezione antivirus e antispyware. Verrà visualizzata la finestra di dialogo **Disattiva temporaneamente la protezione** con il menu a discesa **Intervallo di tempo**. Nel menu a discesa **Intervallo di tempo** viene visualizzato il periodo di tempo in cui la protezione sarà disattivata. Fare clic su **OK** per confermare.

Configurazione controllo computer... - Fare clic per regolare i parametri del controllo su richiesta (controllo eseguito manualmente).

4.1.1 Protezione antivirus e antispyware

La Protezione antivirus e antispyware difende il sistema da attacchi dannosi controllando file, messaggi e-mail e comunicazioni su Internet. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di eliminarla: prima bloccandola e poi pulendola, eliminandola o mettendola in quarantena.

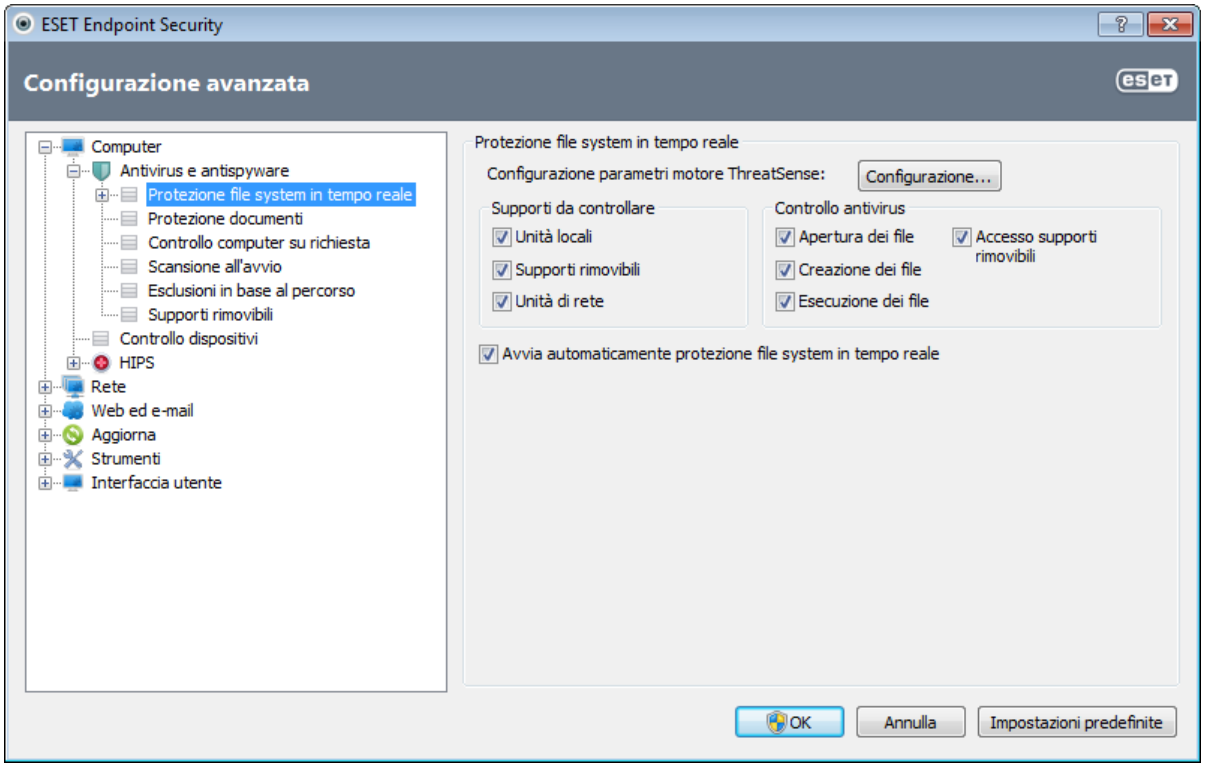
4.1.1.1 Protezione file system in tempo reale

La funzione di Protezione file system in tempo reale consente di controllare tutti gli eventi correlati all'antivirus nel sistema. Tutti i file vengono sottoposti a controllo alla ricerca di codice dannoso nel momento in cui vengono aperti, creati o eseguiti sul computer. La funzione Protezione file system in tempo reale viene avviata all'avvio del sistema.

La funzione Protezione file system in tempo reale controlla tutti i tipi di supporto quando si verificano determinati eventi di sistema, ad esempio l'accesso a un file. Grazie ai metodi di rilevamento della tecnologia ThreatSense (descritti nella sezione Configurazione parametri motore ThreatSense), la Protezione file system in tempo reale potrebbe variare rispetto ai file appena creati o a quelli esistenti. Nel caso di file appena creati è possibile applicare un livello di controllo maggiore.

Per ridurre al minimo l'impatto sul sistema quando si utilizza la protezione in tempo reale, i file già sottoposti a controllo non vengono controllati ripetutamente, a meno che non siano stati modificati. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali. Questo comportamento viene configurato mediante la funzione **Ottimizzazione Smart**. Quando questa funzione è disattivata, tutti i file vengono controllati a ogni accesso. Per modificare questa opzione, premere F5 per aprire la finestra Configurazione avanzata e fare clic su **Computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale** nella struttura Configurazione avanzata. Selezionare quindi il pulsante **Configurazione...** accanto a **Configurazione parametri motore ThreatSense**, fare clic su **Altro** e selezionare o deselezionare l'opzione **Attiva ottimizzazione Smart**.

In base alle impostazioni predefinite, la Protezione file system in tempo reale viene avviata automaticamente all'avvio del sistema operativo e fornisce un controllo ininterrotto. In casi particolari (ad esempio, in caso di conflitto con un altro scanner in tempo reale), la protezione in tempo reale può essere arrestata disattivando l'opzione **Avvia automaticamente la protezione file system in tempo reale**.



4.1.1.1.1 Supporti da controllare

Per impostazione predefinita, vengono controllati tutti i tipi di supporto alla ricerca di eventuali minacce.

Dischi locali - Consente di controllare tutti gli hard disk del sistema.

Dischi rimovibili - Dischetti, CD/DVD, supporti di archiviazione USB e così via.

Dischi di rete - Consente di eseguire la scansione di tutte le unità mappate.

Si consiglia di mantenere le impostazioni predefinite e di modificarle solo in casi specifici, ad esempio quando il controllo di alcuni supporti rallenta notevolmente il trasferimento dei dati.

4.1.1.1.2 Controllo al verificarsi di un evento

Per impostazione predefinita, tutti i file sono sottoposti a scansione all'apertura, durante la creazione o l'esecuzione. È consigliabile mantenere le impostazioni predefinite che offrono il massimo livello di protezione in tempo reale per il computer.

Apertura dei file - Attiva/disattiva la scansione dei file aperti.

Creazione dei file - Attiva/disattiva la scansione dei file appena creati o modificati.

Esecuzione dei file - Attiva/disattiva la scansione dei file eseguiti.

Accesso supporti rimovibili - Consente di attivare o disattivare il controllo avviato accendendo a determinati supporti rimovibili con spazio di archiviazione.

4.1.1.1.3 Opzioni avanzate di controllo

In **Computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale** > **Configurazione avanzata** sono disponibili opzioni di configurazione più dettagliate.

Parametri ThreatSense aggiuntivi per i file appena creati e modificati - I file appena creati hanno maggiore possibilità di essere infettati rispetto a quelli esistenti. Per questo motivo il programma controlla tali file con parametri aggiuntivi. Oltre ai comuni metodi di controllo basati sulle firme, viene utilizzata la funzione di euristica avanzata che consente un notevole miglioramento delle percentuali di rilevamento in quanto l'euristica è in grado di rilevare le nuove minacce prima che l'aggiornamento del database delle firme antivirali venga rilasciato. Oltre che sui file appena creati, il controllo viene eseguito anche sui file autoestraenti (SFX) e sugli eseguibili compressi, ovvero file eseguibili compressi a livello interno. Per impostazione predefinita, gli archivi vengono analizzati fino al 10° livello di nidificazione e controllati indipendentemente dalla loro dimensione effettiva. Per modificare le impostazioni di scansione dell'archivio, deselezionare l'opzione **Impostazioni predefinite scansione degli archivi**.

Parametri ThreatSense aggiuntivi per i file eseguiti - Per impostazione predefinita, quando i file vengono eseguiti non viene usata l'euristica avanzata. In alcuni casi potrebbe tuttavia essere utile attivare questa opzione (selezionando l'opzione **Euristica avanzata all'esecuzione dei file**). È possibile che l'euristica avanzata rallenti l'esecuzione di alcuni programmi a causa dell'aumento dei requisiti di sistema. Se l'opzione **Euristica avanzata all'esecuzione dei file dai dispositivi esterni** è attivata e si desidera escludere alcune porte dei supporti rimovibili (USB) dal controllo con euristica avanzata all'esecuzione dei file, fare clic su **Eccezioni...** per aprire la finestra di esclusioni dei supporti rimovibili. In questa finestra è possibile personalizzare le impostazioni selezionando o deselezionando le caselle di controllo relative a ogni porta.

4.1.1.1.4 Livelli di pulizia

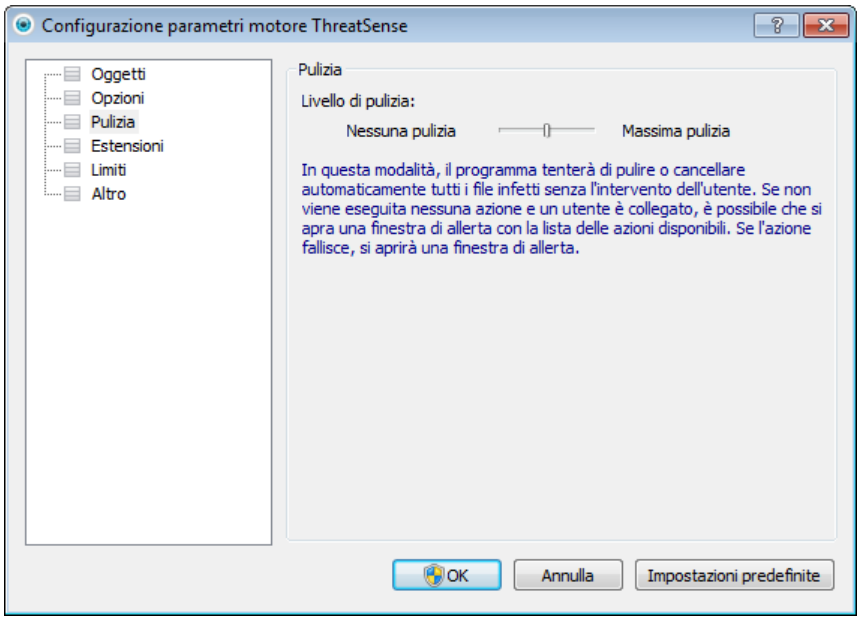
La protezione in tempo reale prevede tre livelli di pulizia (per accedervi, selezionare il pulsante **Configurazione...** nella sezione **Protezione file system in tempo reale** e fare clic sulla sottostruttura **Pulizia**).

Nessuna pulizia - I file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione. Questo livello è indicato per utenti più esperti in grado di eseguire le azioni appropriate in caso di infiltrazione.

Pulitura standard - Il programma tenterà di pulire o eliminare automaticamente un file infetto in base a un'azione predefinita (a seconda del tipo di infiltrazione). Un messaggio nell'angolo in basso a destra della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma offre una scelta di azioni consigliate. Lo stesso si verifica se non è stato possibile completare un'azione predefinita.

Massima pulizia - Il programma pulirà o eliminerà tutti i file infetti. Le uniche eccezioni sono costituite dai file di sistema. Nel caso in cui non sia possibile pulirli, verrà visualizzata una finestra di avviso con la possibilità di scegliere un'azione da eseguire.

Attenzione: se un archivio contiene uno o più file infetti, sono disponibili due opzioni per gestire tale archivio. In modalità standard (Pulitura standard), l'intero archivio viene eliminato se tutti i file in esso contenuti sono infetti. In modalità **Massima pulizia**, l'archivio viene eliminato se contiene almeno un file infetto, indipendentemente dallo stato degli altri file contenuti nell'archivio.


Configurazione parametri motore ThreatSense
Oggetti
Opzioni
Pulizia
Estensioni
Limiti
Altro
Pulizia
Livello di pulizia:
Nessuna pulizia
Massima pulizia
In questa modalità, il programma tenterà di pulire o cancellare automaticamente tutti i file infetti senza l'intervento dell'utente. Se non viene eseguita nessuna azione e un utente è collegato, è possibile che si apra una finestra di allerta con la lista delle azioni disponibili. Se l'azione fallisce, si aprirà una finestra di allerta.
OK
Annulla
Impostazioni predefinite

4.1.1.1.5 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. Prestare la massima attenzione quando si modificano i relativi parametri. È consigliabile modificarli solo in casi specifici, ad esempio se si verifica un conflitto con una determinata applicazione o con lo scanner in tempo reale di un altro programma antivirus.

Dopo l'installazione di ESET Endpoint Security, tutte le impostazioni sono ottimizzate al fine di offrire il massimo livello di protezione del sistema agli utenti. Per ripristinare le impostazioni predefinite, fare clic sul pulsante **Impostazioni predefinite** posizionato in basso a destra della finestra **Protezione file system in tempo reale** (**Configurazione avanzata** > **Computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale**).

4.1.1.1.6 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare un file di test da eicar.com. Questo file di test è un file innocuo, speciale e rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus. Può essere scaricato all'indirizzo http://www.eicar.org/download/eicar.com

NOTA: prima di eseguire un controllo della protezione in tempo reale, è necessario disattivare il firewall. Se il firewall è attivato, rileverà e impedirà di scaricare i file di test.

4.1.1.1.7 Cosa fare se la protezione in tempo reale non funziona

In questo capitolo verranno illustrate situazioni problematiche che potrebbero verificarsi quando si utilizza la protezione in tempo reale e verranno descritte le relative modalità di risoluzione.

La protezione in tempo reale è disattivata

Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, selezionare **Configurazione** nella finestra principale del programma e fare clic su **Protezione file system in tempo reale**.

Se la protezione in tempo reale non viene avviata all'avvio del sistema, è probabile che l'opzione **Avvia automaticamente la protezione file system in tempo reale** sia disattivata. Per attivare l'opzione, accedere a Configurazione avanzata (F5) e fare clic su **Computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale** nella struttura Configurazione avanzata. Nella sezione **Configurazione avanzata** nella parte inferiore della finestra, verificare che la casella di controllo **Avvia automaticamente la protezione file system in tempo reale** sia selezionata.

La protezione in tempo reale non rileva né pulisce le infiltrazioni

Verificare che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema.

La protezione in tempo reale non viene avviata

Se la protezione in tempo reale non viene avviata all'avvio del sistema (e l'opzione **Avvia automaticamente la protezione file system in tempo reale** è attivata), è probabile che entri in conflitto con altri programmi. In questo caso, consultare il Supporto tecnico ESET.

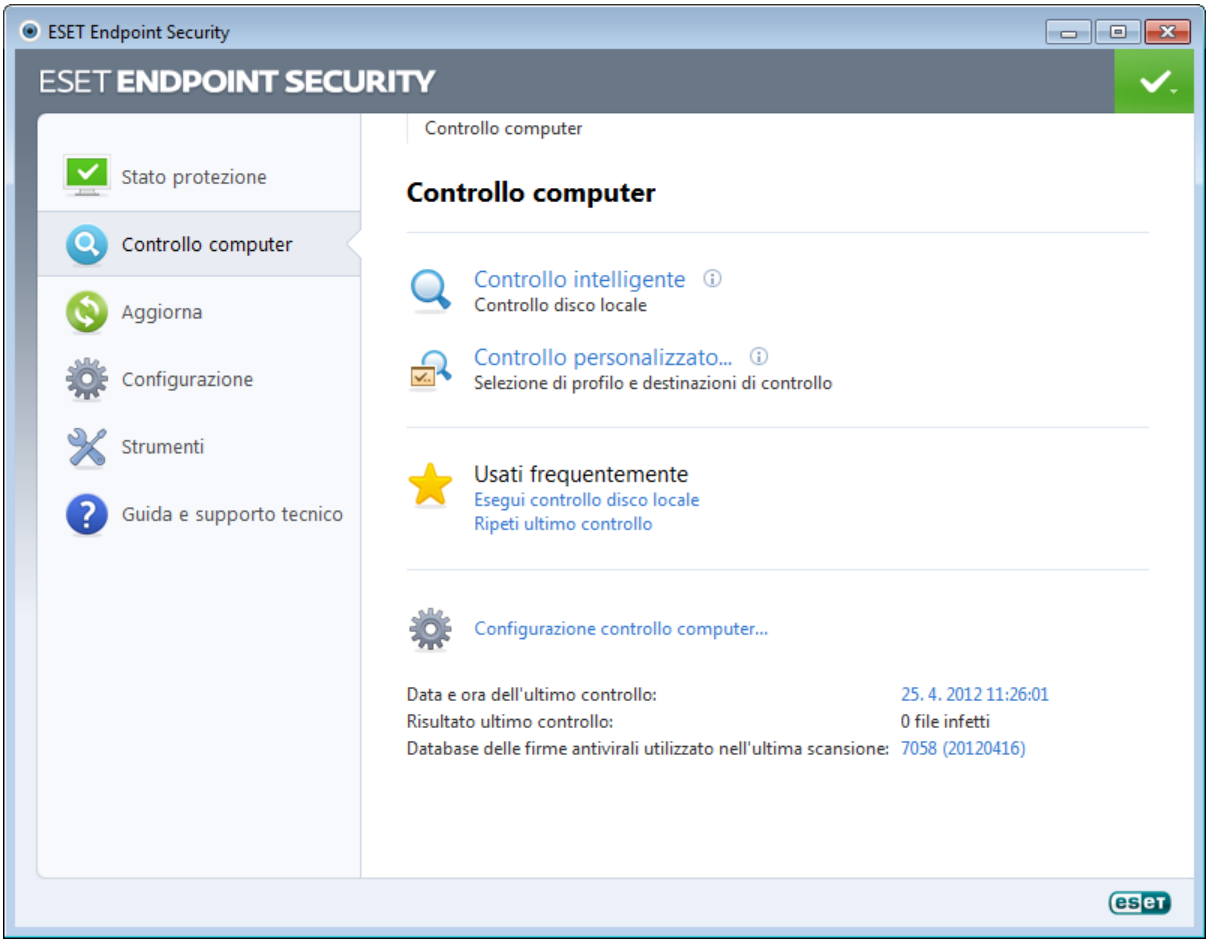
4.1.1.2 Protezione documenti

La funzione Protezione documenti consente di eseguire il controllo dei documenti di Microsoft Office prima della loro apertura e dei file scaricati automaticamente da Internet Explorer, ad esempio gli elementi di Microsoft ActiveX. **Integrazione nel sistema** consente di attivare il sistema di protezione. Per modificare questa opzione, premere F5 per aprire la finestra Configurazione avanzata e fare clic su **Computer** > **Antivirus e antispyware** > **Protezione documenti** nella struttura Configurazione avanzata. Se attivata, la Protezione documenti è visualizzabile nella finestra principale del programma di ESET Endpoint Security in **Configurazione** > **Computer**.

Questa funzione è attivata dalle applicazioni che utilizzano Microsoft Antivirus API (ad esempio Microsoft Office 2000 e versioni successive o Microsoft Internet Explorer 5.0 e versioni successive).

4.1.1.3 Controllo computer

Lo scanner su richiesta è una parte importante della soluzione antivirus. Viene utilizzato per eseguire il controllo di file e di cartelle sul computer in uso. Dal punto di vista della protezione, è essenziale che le scansioni del computer non vengano eseguite solo quando si sospetta un'infezione, ma periodicamente, nell'ambito delle normali misure di protezione. Si consiglia di eseguire periodicamente controlli approfonditi del sistema al fine di rilevare virus che non sono stati rilevati dalla Protezione file system in tempo reale quando sono stati scritti sul disco. Ciò può verificarsi se la Protezione file system in tempo reale era disattivata in quel momento, il database antivirus era obsoleto o il file non è stato rilevato come virus quando salvato sul disco.



Sono disponibili due tipologie di **Controllo computer** **Controllo intelligente**, che consente di eseguire rapidamente la scansione del sistema senza che sia necessario configurare ulteriori parametri. **Controllo personalizzato**, che consente di selezionare uno dei profili di scansione predefiniti, nonché di scegliere oggetti da controllare specifici.

Per ulteriori informazioni sul processo di scansione, consultare il capitolo Avanzamento scansione.

È consigliabile eseguire un controllo del computer almeno una volta al mese. Il controllo può essere configurato come

attività pianificata in **Strumenti** > **Pianificazione attività**.

4.1.1.3.1 Tipo di controllo

4.1.1.3.1.1 Controllo intelligente

La funzione Controllo intelligente consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il Controllo intelligente è facile da utilizzare e non richiede una configurazione di scansione dettagliata. Il Controllo intelligente consente di effettuare un controllo di tutti i file presenti nei dischi locali, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di pulizia viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di disinfezione, consultare la sezione Disinfezione.

4.1.1.3.1.2 Controllo personalizzato

Il controllo personalizzato è una soluzione ottimale se si desidera specificare parametri di scansione quali oggetti da controllare e metodi di scansione. Il vantaggio del controllo personalizzato è la possibilità di configurare i parametri in dettaglio. È possibile salvare le configurazioni come profili di scansione definiti dagli utenti che risultano particolarmente utili se il controllo viene eseguito più volte con gli stessi parametri.

Per scegliere gli oggetti da controllare, selezionare **Controllo computer** > **Controllo personalizzato**, quindi selezionare un'opzione dal menu a discesa **Oggetti da controllare** oppure selezionare oggetti specifici dalla struttura ad albero. L'oggetto da controllare può anche essere specificato immettendo il percorso della cartella o dei file che si desidera includere nel controllo. Se si desidera controllare solo il sistema senza ulteriori azioni di pulizia, selezionare l'opzione **Controllo senza rimozione**. È inoltre possibile scegliere tra tre livelli di disinfezione selezionando **Configurazione...** > **Pulizia**.

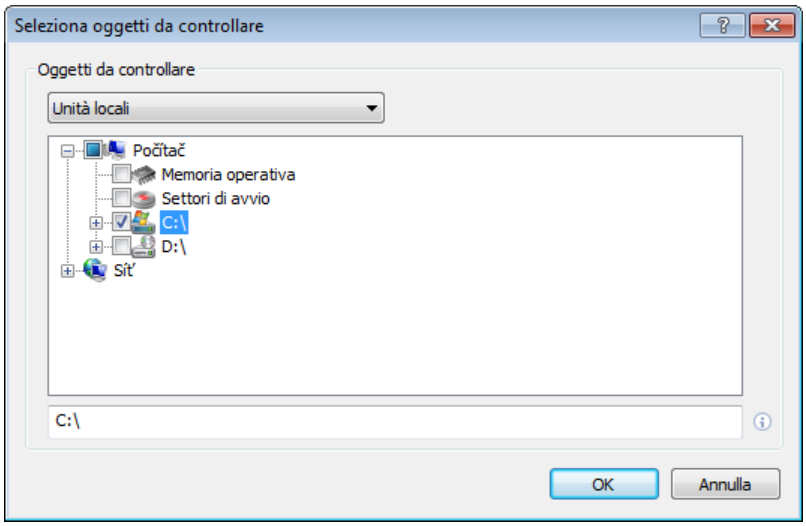
L'esecuzione di controlli del computer attraverso il controllo personalizzato è un'operazione raccomandata per gli utenti avanzati con precedenti esperienze di utilizzo di programmi antivirus.

4.1.1.3.2 Oggetti da controllare

La finestra Oggetti da controllare consente di definire gli oggetti (memoria, unità, settori, file e cartelle) che verranno sottoposti a controllo alla ricerca di infiltrazioni. Il menu a discesa **Oggetti da controllare** consente di selezionare gli oggetti da controllare predefiniti.

- **Attraverso le impostazioni di profilo** - Consente di selezionare le destinazioni nel profilo di controllo selezionato.
- **Supporti rimovibili** - Consente di selezionare dischetti, supporti di archiviazione USB, CD/DVD.
- **Unità locali** - Consente di selezionare tutti gli hard disk del sistema.
- **Unità di rete** - Consente di selezionare tutte le unità di rete mappate.
- **Nessuna selezione** - Consente di annullare tutte le selezioni.

Una destinazione di scansione può anche essere specificata immettendo il percorso della cartella o dei file che si desidera includere nel controllo. Selezionare gli oggetti dalla struttura ad albero contenente un elenco di tutti i supporti disponibili nel computer.



Per visualizzare rapidamente una destinazione selezionata o per aggiungere direttamente una destinazione desiderata, inserirla nel campo vuoto sotto l'elenco delle cartelle. Ciò è possibile solo se nella struttura ad albero non sono stati selezionati oggetti e il menu **Oggetti da controllare** è impostato su **Nessuna selezione**.

4.1.1.3.3 Profili di controllo

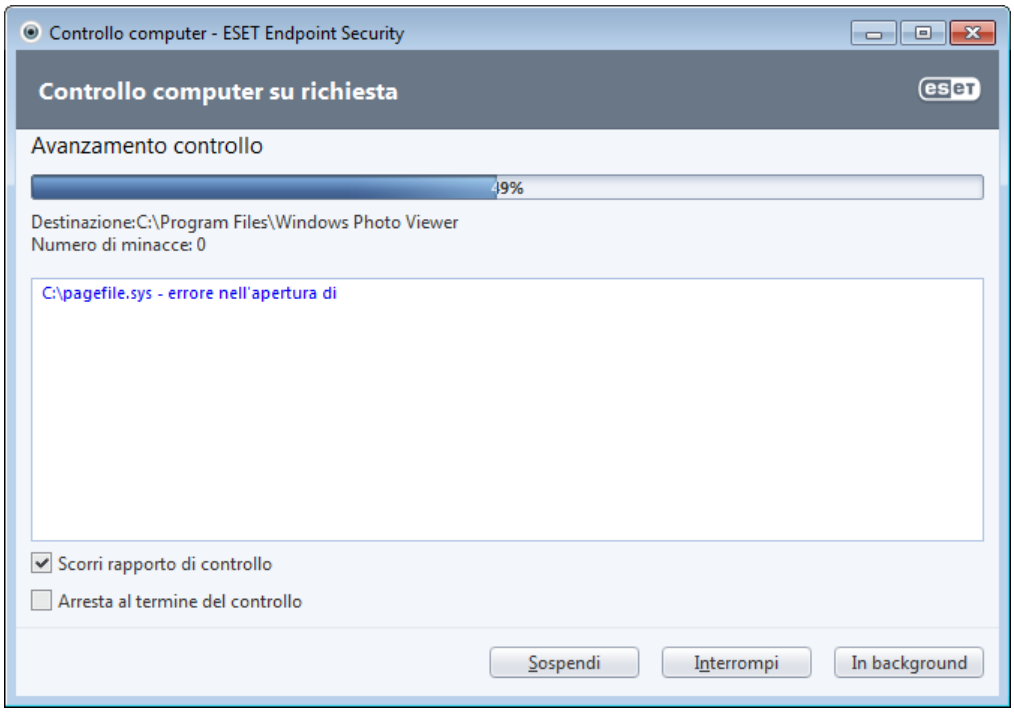
È possibile salvare i parametri di scansione preferiti per i controlli futuri. È consigliabile creare un profilo di scansione differente (con diversi oggetti da controllare, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Computer** > **Antivirus e antispyware** > **Controllo computer** > **Profili...**. Nella finestra **Profili di configurazione** è disponibile un menu a discesa **Profili selezionati** contenente i profili di scansione esistenti e l'opzione per crearne di nuovi. Per ricevere assistenza nella creazione di un profilo di scansione adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione della scansione.

Esempio: si supponga di voler creare il proprio profilo di scansione e che la configurazione del Controllo intelligente sia appropriata solo in parte, in quanto non si desidera eseguire la scansione di eseguibili compressi o di applicazioni potenzialmente pericolose, bensì si intende applicare l'opzione **Massima pulizia**. Nella finestra **Profili di configurazione**, fare clic sul pulsante **Aggiungi...**. Immettere il nome del nuovo profilo nel campo **Nome profilo**, quindi selezionare **Controllo intelligente** dal menu a discesa **Copia impostazioni dal profilo**. Regolare quindi gli altri parametri in base ai requisiti specifici.

4.1.1.3.4 Avanzamento controllo

Nella finestra di avanzamento del controllo viene mostrato lo stato attuale del controllo e informazioni sul numero di file rilevati che contengono codice dannoso.



NOTA: è normale che alcuni file, ad esempio file protetti con password o file che vengono utilizzati esclusivamente dal sistema (in genere il file pagefile.sys e alcuni file di registro), non possano essere sottoposti al controllo.

Avanzamento controllo - La barra di avanzamento mostra la percentuale di oggetti già sottoposti a controllo rispetto a quelli in attesa di essere sottoposti al controllo. Il valore è derivato in base al numero totale di oggetti inclusi nel controllo.

Destinazione - Nome dell'oggetto in fase di controllo e relativo percorso.

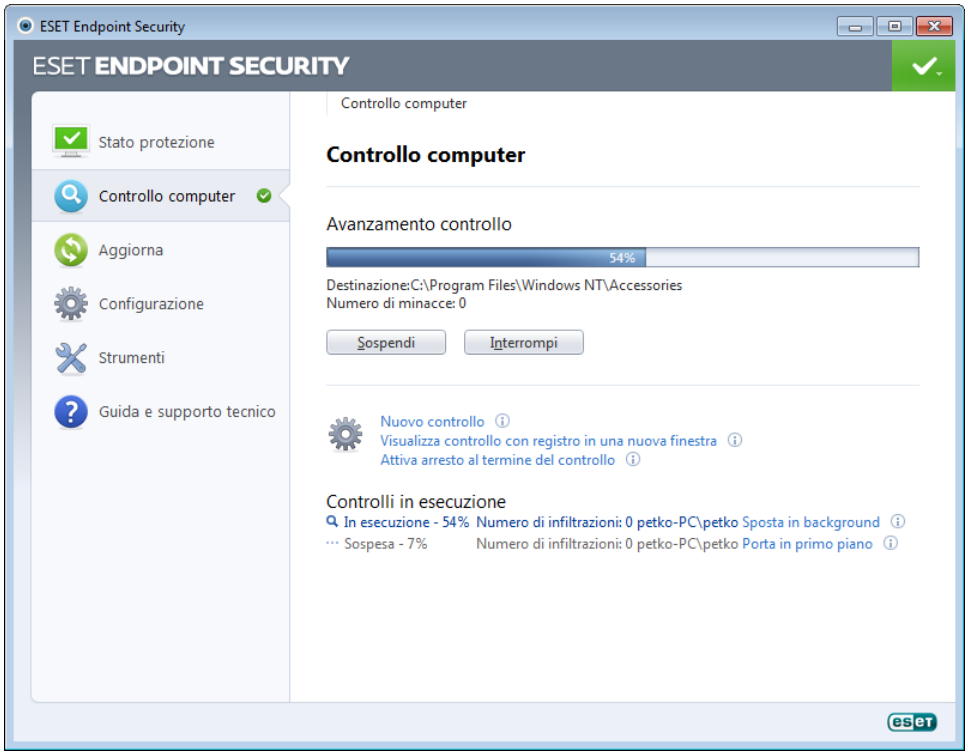
Numero di minacce - Mostra il numero totale di minacce rilevate durante un controllo.

Sospendi - Sospende un controllo.

Riprendi - Questa opzione è visibile quando l'avanzamento controllo è sospeso. Fare clic su **Riprendi** per continuare il controllo.

Interrompi - Interrompe il controllo.

In background - Consente di eseguire un altro controllo parallelo. Il controllo in esecuzione verrà ridotto in background.



Fare clic su **Porta in primo piano** per portare un controllo in primo piano e ritornare al processo di scansione.

Scorri rapporto di scansione - Se questa opzione è attivata, il rapporto di scansione scorrerà automaticamente quando vengono aggiunte nuove voci in modo da rendere visibili le voci più recenti.

Attiva arresto al termine del controllo - Attiva un arresto pianificato al termine del controllo su richiesta del computer. Verrà visualizzata una finestra di dialogo in cui viene richiesto all'utente di confermare l'arresto entro 60 secondi. Fare clic su **Annulla** per annullare l'arresto richiesto.

4.1.1.4 Controllo all'avvio

All'avvio del sistema o in fase di aggiornamento del database delle firme antivirali verrà eseguito il controllo automatico del file di avvio. Questo controllo dipende dalla configurazione di Pianificazione configurazione e attività.

Le opzioni di controllo all'avvio fanno parte della pianificazione dell'attività **Controllo del file di avvio del sistema**. Per modificarne le impostazioni, accedere a **Strumenti** > **Pianificazione attività**, fare clic su **Controllo automatico file di avvio** e sul pulsante **Modifica...**. Nell'ultimo passaggio verrà visualizzata la finestra Controllo automatico file di avvio (per ulteriori informazioni, vedere il capitolo seguente).

Per ulteriori informazioni sulla creazione e sulla gestione di Pianificazione attività, vedere Creazione di nuove attività.

4.1.1.4.1 Controllo automatico file di avvio

Il menu a discesa **Livello di controllo** consente di specificare il livello di controllo dei file eseguiti all'avvio del sistema. I file sono visualizzati in ordine crescente in base al numero di file da sottoporre al controllo:

- **Solo i file utilizzati più di frequente** (ultimi file sottoposti al controllo)
- **File utilizzati di frequente**
- **File utilizzati comunemente**
- **File utilizzati raramente**
- **Tutti i file registrati** (la maggior parte dei file sottoposti al controllo)

Sono inoltre inclusi due gruppi del **Livello di controllo** specifici:

- **File eseguiti prima dell'accesso utente** - Contiene file da posizioni che ne consentono l'esecuzione senza che l'utente abbia eseguito l'accesso (include quasi tutte le posizioni di avvio quali servizi, oggetti browser helper, notifiche Winlogon, voci della pianificazione attività di Windows, dll noti e così via).
- **File eseguiti dopo l'accesso utente** - Contiene file da posizioni che ne consentono l'esecuzione solo dopo che l'utente ha eseguito l'accesso (include file che sono eseguiti solo per un utente specifico, in genere i file in

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run)

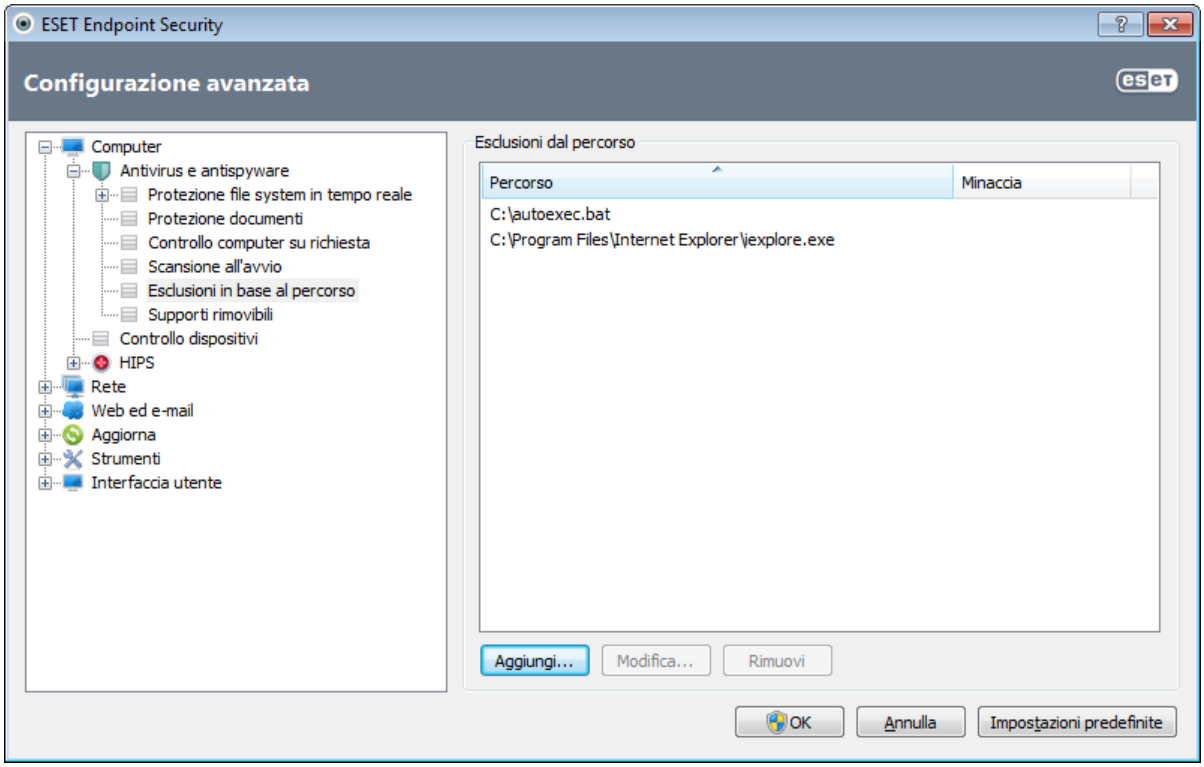
Per ogni gruppo, vengono definiti elenchi di file da sottoporre al controllo.

Priorità di controllo - Un livello di priorità da utilizzare per l'avvio del controllo:

- **Normale** (con un carico di sistema medio),
- **Basso** (con un carico di sistema basso),
- **Più basso** (quando il carico di sistema è più basso possibile),
- **Quando inattivo** (l'attività verrà eseguita solo quando il sistema è inattivo).

4.1.1.5 Esclusioni dal percorso

Le esclusioni consentono di escludere file e cartelle dalla scansione. Non è consigliabile modificare queste opzioni per garantire che la scansione per il rilevamento delle minacce venga eseguita su tutti gli oggetti. In alcuni casi è tuttavia necessario escludere un oggetto. Ad esempio, le voci di database di grandi dimensioni che rallenterebbero il computer durante la scansione o software che entra in conflitto con la scansione.



Percorso - Percorso dei file e delle cartelle esclusi.

Minaccia - Se è presente il nome di una minaccia accanto a un file escluso, significa che il file viene escluso solo per la minaccia indicata e non per tutte. Quindi se il file si infetta successivamente con altri malware, verrà rilevato dal modulo antivirus. Questo tipo di esclusione può essere utilizzato solo per alcuni tipi di infiltrazioni e può essere creato nella finestra di avviso Minaccia che segnala l'infiltrazione (fare clic su **Mostra impostazioni avanzate** e selezionare **Escludi dal rilevamento**) o in **Imposta** > **Quarantena** utilizzando l'opzione del menu contestuale **Ripristina ed escludi dal rilevamento** sul file in quarantena.

Aggiungi... - Esclude gli oggetti dal rilevamento.

Modifica... - Consente di modificare le voci selezionate.

Rimuovi - Rimuove le voci selezionate.

Per escludere un oggetto dalla scansione:

1. Fare clic su **Aggiungi...**,
2. Immettere il percorso di un oggetto oppure selezionarlo nella struttura ad albero.

È possibile utilizzare i caratteri jolly per includere un gruppo di file. Un punto interrogativo (?) rappresenta un carattere variabile singolo, mentre un asterisco (*) rappresenta una stringa variabile di zero o più caratteri.

Esempi

- Se si desidera escludere tutti i file presenti in una cartella, digitare il percorso della cartella e utilizzare la maschera "*.*".
- Per escludere un'unità intera, compresi tutti i file e le sottocartelle, usare la maschera "D:*".
- Se si desidera escludere solo i file DOC, utilizzare la maschera "*.doc".
- Se il nome di un file eseguibile contiene un determinato numero di caratteri (e i caratteri variano) e si è sicuri solo della prima lettera (ad esempio "D"), utilizzare il formato seguente: "D????.exe". I punti interrogativi sostituiscono i caratteri mancanti (sconosciuti).

4.1.1.6 Configurazione parametri motore ThreatSense

ThreatSense è una tecnologia costituita da numerosi metodi complessi di rilevamento delle minacce. Questa tecnologia è proattiva, ovvero fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Utilizza una combinazione di diversi metodi (analisi del codice, emulazione del codice, firme generiche, firme antivirali) che operano in modo integrato per potenziare in modo significativo la protezione del sistema. Il motore di scansione è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di configurazione della tecnologia ThreatSense consentono di specificare vari parametri di scansione:

- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di pulizia e così via.

Per aprire la finestra di impostazione, fare clic sul pulsante **Configurazione...** presente in qualsiasi finestra di impostazione del modulo che utilizza la tecnologia ThreatSense (vedere di seguito). Scenari di protezione diversi possono richiedere configurazioni diverse. In considerazione di questo, ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- Protezione file system in tempo reale
- Protezione documenti
- Protezione client e-mail
- Protezione accesso Web,
- e Controllo computer.

I parametri ThreatSense sono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica dei parametri per il controllo degli eseguibili compressi o per consentire il controllo con l'euristica avanzata nel modulo di protezione del file system in tempo reale potrebbe causare un rallentamento del sistema (in genere solo i file appena creati sono sottoposti a controllo con questi metodi). È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, ad eccezione di Controllo computer.

4.1.1.6.1 Oggetti

Nella sezione **Oggetti** è possibile definire i componenti e file del computer che saranno sottoposti a scansione per la ricerca di infiltrazioni.

Memoria operativa - Consente di eseguire la scansione per la ricerca di minacce che attaccano la memoria operativa del sistema.

Settori di avvio - Consente di controllare i settori di avvio alla ricerca di virus nel record di avvio principale.

File di e-mail - Il programma supporta le estensioni seguenti: DBX (Outlook Express) ed EML.

Archivi - Il programma supporta le estensioni seguenti: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e molti altri ancora.

Archivi autoestraenti - Gli archivi autoestraenti (SFX) sono archivi che non necessitano di programmi speciali, ovvero archivi, per decomprimersi.

Eseguibili compressi - Dopo l'esecuzione, gli eseguibili compressi (diversamente dai tipi di archivio standard) si decomprimono nella memoria. Oltre ai programmi statici standard (UPS, yoda, ASPack, FSG e così via), lo scanner supporta (grazie all'emulazione del codice) numerosi altri tipi di programmi di compressione.

4.1.1.6.2 Opzioni

La sezione **Opzioni** consente di selezionare i metodi utilizzati durante una scansione del sistema per il rilevamento di eventuali infiltrazioni. Sono disponibili le seguenti opzioni:

Euristica - L'euristica è un algoritmo che analizza l'attività (dannosa) dei programmi. Il vantaggio principale offerto consiste nella capacità di identificare software dannoso precedentemente inesistente o non conosciuto dal database delle firme antivirali precedente. Lo svantaggio è una probabilità (minima) di falsi allarmi.

Euristica avanzata/DNA/Firme Smart - L'euristica avanzata si basa su un esclusivo algoritmo di euristica sviluppato da ESET, ottimizzato per il rilevamento dei worm e dei trojan horse e scritto in linguaggi di programmazione di alto livello. Grazie all'euristica avanzata, le capacità di rilevamento del programma sono significativamente più elevate. Le firme possono rilevare e identificare i virus in modo affidabile. Grazie al sistema di aggiornamento automatico, le nuove firme sono disponibili entro poche ore dal rilevamento di una minaccia. Lo svantaggio delle firme è costituito dal fatto che rilevano solo i virus conosciuti o con leggere modifiche rispetto all'originale.

Le **applicazioni potenzialmente indesiderate** (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- Nuove finestre mai visualizzate in precedenza (popup, annunci pubblicitari)
- Attivazione ed esecuzione di processi nascosti
- Maggiore utilizzo delle risorse del sistema
- Modifiche dei risultati di ricerca
- Applicazioni che comunicano con server remoti.

Applicazioni potenzialmente pericolose - Applicazioni potenzialmente pericolose è la classificazione utilizzata per il software legale e commerciale. Sono inclusi programmi quali gli strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente). Questa opzione è disattivata per impostazione predefinita.

ESET Live Grid - Grazie alla tecnologia di reputazione di ESET, le informazioni sui file controllati vengono verificate rispetto ai dati di ESET Live Grid basato sul cloud allo scopo di migliorare il rilevamento e la velocità di controllo.

4.1.1.6.3 Pulizia

Le impostazioni di disinfezione determinano il comportamento dello scanner durante la disinfezione di file infetti. Sono disponibili 3 livelli di disinfezione:

Nessuna pulizia - I file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione. Questo livello è indicato per utenti più esperti in grado di eseguire le azioni appropriate in caso di infiltrazione.

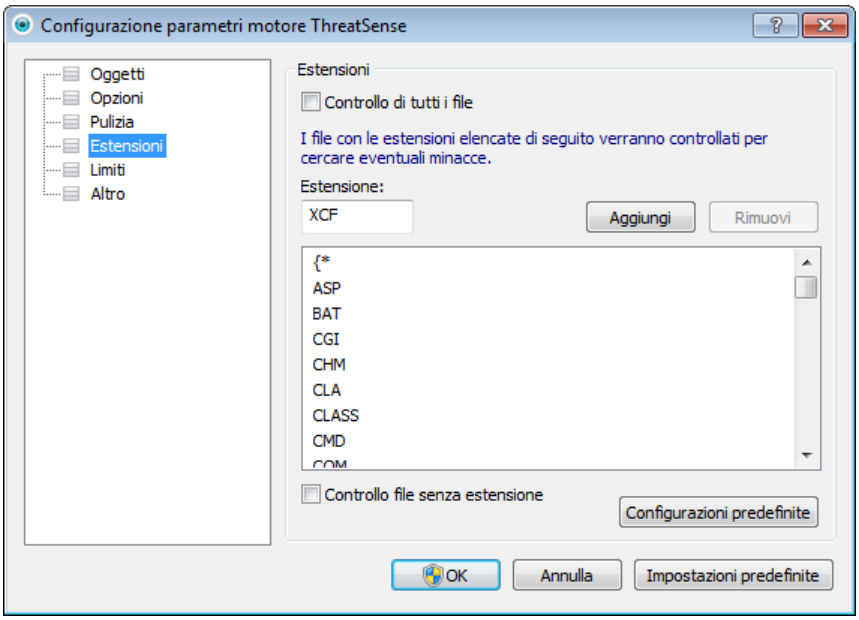
Pulitura standard - Il programma tenterà di pulire o eliminare automaticamente un file infetto in base a un'azione predefinita (a seconda del tipo di infiltrazione). Un messaggio nell'angolo in basso a destra della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma offre una scelta di azioni consigliate. Lo stesso si verifica se non è stato possibile completare un'azione predefinita.

Massima pulizia - Il programma pulirà o eliminerà tutti i file infetti. Le uniche eccezioni sono costituite dai file di sistema. Nel caso in cui non sia possibile pulirli, verrà visualizzata una finestra di avviso con la possibilità di scegliere un'azione da eseguire.

Attenzione: se un archivio contiene uno o più file infetti, sono disponibili due opzioni per gestire tale archivio. In modalità standard (Pulitura standard), l'intero archivio viene eliminato se tutti i file in esso contenuti sono infetti. In modalità **Massima pulizia**, l'archivio viene eliminato se contiene almeno un file infetto, indipendentemente dallo stato degli altri file contenuti nell'archivio.

4.1.1.6.4 Estensione

Un'estensione è una parte del nome di un file delimitata da un punto. Un'estensione definisce il tipo e il contenuto di un file. Questa sezione delle impostazioni parametri ThreatSense consente di definire i tipi di file da sottoporre a controllo.



Per impostazione predefinita, tutti i file vengono sottoposti a scansione indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dalla scansione. Se l'opzione **Scansione di tutti i file** è deselezionata, l'elenco viene modificato per mostrare le estensioni di tutti i file sottoposti attualmente alla scansione.

Per attivare la scansione dei file senza estensione, selezionare l'opzione **Scansione file senza estensione**. L'opzione **Non eseguire scansione dei file senza estensione** diventa disponibile quando si seleziona l'opzione **Controllo di tutti i file**.

L'esclusione di file è utile nel caso in cui il controllo di determinati tipi di file impedisse il corretto funzionamento di un programma che utilizzi le estensioni. Ad esempio, potrebbe essere consigliabile escludere le estensioni EDB, EML e TMP durante l'utilizzo dei server Microsoft Exchange.

I pulsanti **Aggiungi** e **Rimuovi** consentono di attivare o impedire la scansione di estensioni di file specifiche. Digitando un'**Estensione** si attiva il pulsante **Aggiungi** che consente di aggiungere la nuova estensione all'elenco. Per eliminare un'estensione dall'elenco, selezionarla quindi fare clic sul pulsante **Rimuovi**.

È possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri, mentre il punto interrogativo sostituisce qualsiasi simbolo. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, poiché l'elenco deve contenere solo indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente.

Per eseguire solo il controllo del gruppo di estensioni predefinito, fare clic sul pulsante **Impostazioni predefinite**, quindi selezionare **Sì** per confermare.

4.1.1.6.5 Limiti

La sezione Limiti consente di specificare la dimensione massima degli oggetti e i livelli di nidificazione degli archivi sui quali eseguire la scansione:

Dimensioni massima oggetto - Determina la dimensione massima degli oggetti su cui eseguire la scansione. Il modulo antivirus eseguirà unicamente la scansione degli oggetti di dimensioni inferiori a quelle specificate. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di dimensioni maggiori dalla scansione. Il valore predefinito è: illimitato.

Durata massima scansione dell'oggetto (sec.) - Consente di definire il valore massimo di tempo destinato alla scansione di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà la scansione dell'oggetto una volta raggiunto tale valore, indipendentemente dal fatto che la scansione sia stata completata. Il valore predefinito è: illimitato.

Livello di nidificazione degli archivi - Specifica il livello massimo di scansione degli archivi. Il valore predefinito è: 10.

Dimensioni massima file in archivio - Questa opzione consente di specificare le dimensioni massime dei file contenuti all'interno degli archivi, i quali, una volta estratti, saranno sottoposti a scansione. Il valore predefinito è: illimitato.

Se per tali motivi la scansione viene terminata anticipatamente, la casella di controllo dell'archivio non verrà selezionata.

Nota: si consiglia di non modificare i valori predefiniti. In circostanze normali, non sussiste alcun motivo per farlo.

4.1.1.6.6 Altro

Nella sezione **Altro** è possibile configurare le seguenti opzioni:

Registra tutti gli oggetti - Se questa opzione è selezionata, il file di rapporto riporta tutti i file sottoposti a scansione, anche quelli non infetti. Se ad esempio viene individuata un'infiltrazione all'interno di un archivio, nel rapporto verranno elencati anche i file puliti presenti all'interno dell'archivio.

Attiva ottimizzazione Smart - Al fine di garantire il miglior livello di scansione, l'attivazione dell'ottimizzazione Smart consente l'utilizzo delle impostazioni più efficienti alla velocità di scansione più elevata. I vari moduli di protezione eseguono la scansione in modo intelligente, utilizzando metodi di scansione differenti e applicandoli a tipi di file specifici. Se l'opzione di ottimizzazione Smart non è attivata, durante la scansione vengono applicate solo le impostazioni definite dall'utente nell'architettura ThreatSense di moduli specifici.

Quando si configurano i parametri del motore ThreatSense per l'esecuzione di un Controllo computer, sono disponibili le seguenti opzioni:

Flussi di dati alternativi (ADS) - I flussi di dati alternativi utilizzati dal file system NTFS sono associazioni di file e cartelle invisibili alle tecniche di scansione standard. Molte infiltrazioni cercano di non essere rilevate presentandosi come flussi di dati alternativi.

Esegui scansioni in background con priorità bassa - Ogni sequenza di scansione utilizza una determinata quantità di risorse del sistema. Se si utilizzano programmi che necessitano di molte risorse di sistema, è possibile attivare la scansione in background con priorità bassa e risparmiare risorse per le applicazioni.

Mantieni timestamp ultimo accesso - Selezionare questa opzione per mantenere la data e l'ora di accesso originali ai file su cui è stata eseguita la scansione anziché aggiornarli (ad esempio, per l'utilizzo di sistemi di backup dei dati).

Scorri rapporto di controllo - Questa opzione consente di abilitare/disabilitare lo scorrimento del rapporto. Se viene selezionata, è possibile scorrere le informazioni verso l'alto nella finestra di visualizzazione.

4.1.1.7 Rilevamento di un'infiltrazione

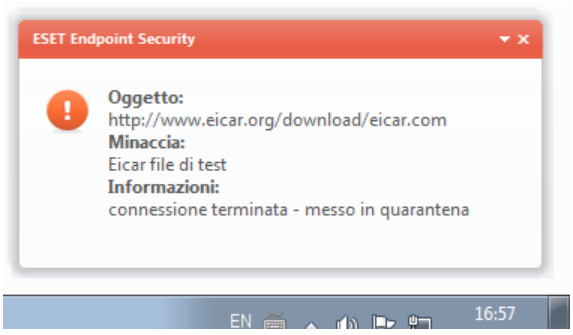
Le infiltrazioni possono raggiungere il sistema da diversi accessi, ad esempio pagine Web, cartelle condivise, messaggi e-mail o dispositivi rimovibili (USB, dischi esterni, CD, DVD, dischetti e così via).

Comportamento standard

In linea generale, ESET Endpoint Security gestisce le infiltrazioni rilevandole mediante

- Protezione file system in tempo reale
- Protezione accesso Web,
- Protezione client e-mail o
- Controllo computer su richiesta

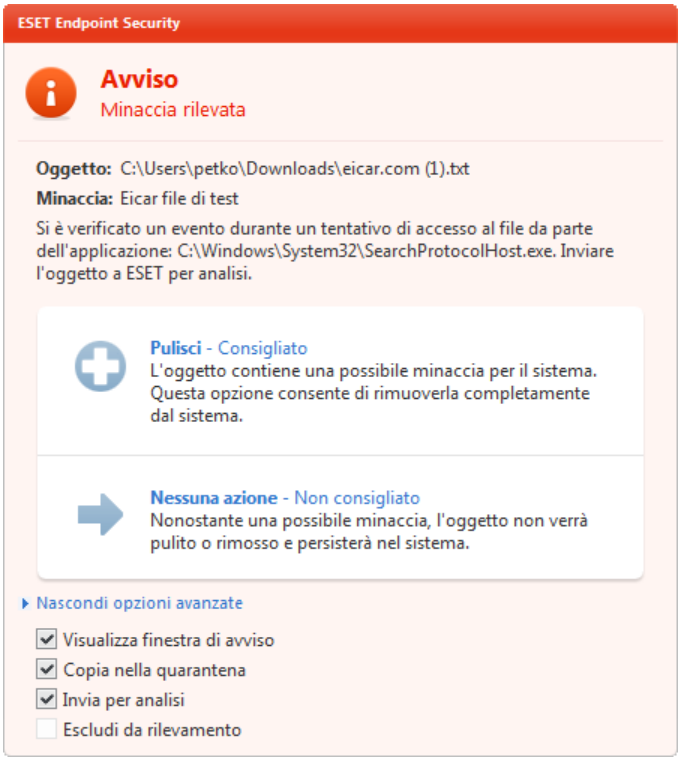
Ciascuna di tali opzioni utilizza il livello di pulitura standard e tenta di pulire il file e spostarlo nella Quarantena o interrompere la connessione. Una finestra di avviso viene visualizzata nell'area di notifica posta nell'angolo in basso a destra della schermata. Per ulteriori informazioni sui livelli di pulizia e sul comportamento, vedere Pulizia.



Pulizia ed eliminazione

In assenza di azioni predefinite per l'esecuzione della Protezione file system in tempo reale, verrà chiesto all'utente di selezionare un'opzione in una finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione** in quanto i file infettati non verranno puliti. È opportuno selezionare questa opzione solo quando si è certi che un file non è pericoloso e che si tratta di un errore di rilevamento.

Applicare la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto un codice dannoso al file. In tal caso, tentare innanzitutto di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codice dannoso, verrà eliminato.


ESET Endpoint Security
Avviso
Minaccia rilevata
Oggetto: C:\Users\petko\Downloads\eicar.com (1).txt
Minaccia: Eicar file di test
Si è verificato un evento durante un tentativo di accesso al file da parte dell'applicazione: C:\Windows\System32\SearchProtocolHost.exe. Inviare l'oggetto a ESET per analisi.
Pulisci - Consigliato
L'oggetto contiene una possibile minaccia per il sistema. Questa opzione consente di rimuoverla completamente dal sistema.
Nessuna azione - Non consigliato
Nonostante una possibile minaccia, l'oggetto non verrà pulito o rimosso e persisterà nel sistema.
Nascondi opzioni avanzate
Visualizza finestra di avviso
Copia nella quarantena
Invia per analisi
Escludi da rilevamento

Se un file infetto è "bloccato" o utilizzato da un processo del sistema, verrà eliminato solo dopo essere stato rilasciato (generalmente dopo il riavvio del sistema).

Eliminazioni dei file negli archivi

In modalità di pulizia predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati nel caso in cui dovessero contenere anche file puliti non dannosi. È consigliabile essere prudenti durante l'esecuzione di un controllo di massima pulizia: con tale modalità di pulitura l'archivio verrà eliminato nel caso in cui contenga almeno un file infetto, indipendentemente dallo stato degli altri file dell'archivio.

Se il computer mostra segnali di infezione malware, ad esempio appare più lento, si blocca spesso e così via, è consigliabile attenersi alle seguenti istruzioni:

- Aprire ESET Endpoint Security e fare clic su Controllo computer,
- Fare clic su **Controllo intelligente** (per ulteriori informazioni, consultare Controllo intelligente),
- Al termine della scansione, controllare nel registro il numero di file sottoposti a controllo, file infetti e file puliti.

Se si desidera effettuare il controllo solo di una parte del disco, scegliere **Controllo personalizzato** e selezionare gli oggetti da controllare alla ricerca di virus.

4.1.2 Supporti rimovibili

ESET Endpoint Security offre il controllo automatico dei supporti rimovibili (CD/DVD/USB/...). Questo modulo consente di controllare un supporto inserito. Questa funzionalità può essere utile se l'amministratore del computer desidera impedire l'utilizzo di supporti rimovibili con contenuti non desiderati da parte degli utenti.

Azione da eseguire dopo aver collegato i dispositivi esterni - Selezionare l'azione predefinita che verrà eseguita quando un supporto rimovibile viene inserito nel computer (CD/DVD/USB). Se è selezionata l'opzione **Mostra opzioni di scansione**, verrà visualizzata una notifica che consente di scegliere un'azione desiderata:

- **Controlla ora** - Viene eseguito il controllo del computer su richiesta del supporto rimovibile inserito.
- **Controlla più tardi** - Non verrà eseguita alcuna azione e la finestra **Rilevato nuovo dispositivo** verrà chiusa.
- **Configurazione...** - Consente di accedere alla sezione di configurazione del supporto rimovibile.

In ESET Endpoint Security è inoltre disponibile la funzionalità Controllo dispositivi che consente di definire regole per l'utilizzo dei dispositivi esterni su un determinato computer. Per ulteriori informazioni sul Controllo dispositivi, vedere la sezione Controllo dispositivi.

4.1.3 Controllo dispositivi

ESET Endpoint Security offre il controllo automatico dei dispositivi (CD/DVD/USB/...). Questo modulo consente di controllare, bloccare o regolare i filtri/autorizzazioni e le modalità di accesso e di utilizzo di un determinato dispositivo da parte dell'utente. Questa funzionalità può essere utile se l'amministratore del computer desidera impedire l'utilizzo di dispositivi con contenuti non desiderati da parte degli utenti.

Dispositivi esterni supportati

- CD/DVD/Blu-ray
- Supporto di archiviazione USB
- Dispositivo FireWire
- Dispositivo di acquisizione immagini
- Stampante USB
- Bluetooth
- Lettore di schede
- Modem
- Porta LPT/COM

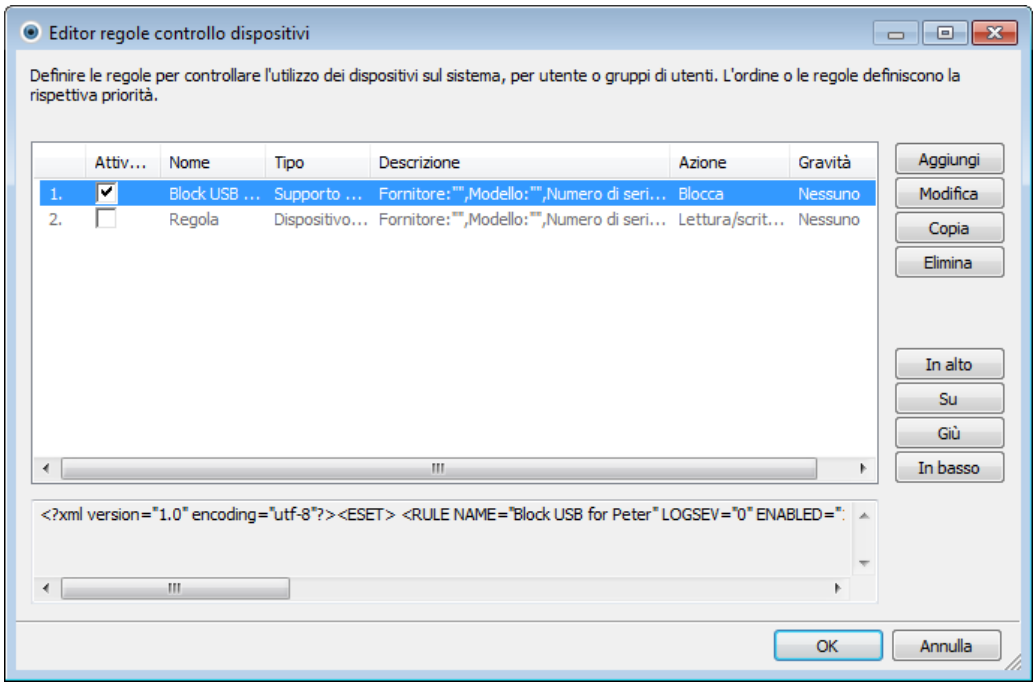
Le opzioni di configurazione del controllo dispositivi possono essere modificate in **Configurazione avanzata** (F5) > **Controllo dispositivi**.

Selezionando la casella di controllo vicino a **Integrazione nel sistema**, è possibile attivare la funzione Controllo dispositivi in ESET Endpoint Security. Per rendere effettive le modifiche, sarà necessario riavviare il computer. Dopo aver attivato la funzione Controllo dispositivi, si attiverà l'opzione **Configura regole...**, che consente di aprire la finestra Editor regole controllo dispositivi.

Se il dispositivo esterno inserito applica una regola esistente che esegue l'azione **Blocca**, nell'angolo in basso a destra comparirà una finestra di notifica e non sarà possibile accedere al dispositivo.

4.1.3.1 Regole controllo dispositivi

Nella finestra **Editor regole controllo dispositivi** sono visualizzate le regole esistenti. In questa finestra è possibile controllare in maniera precisa i dispositivi esterni che gli utenti collegano al computer.



È possibile consentire o bloccare dispositivi specifici in base all'utente o gruppo di utenti e a parametri del dispositivo aggiuntivi che è possibile specificare nella configurazione della regola. L'elenco delle regole contiene diverse descrizioni di una regola quali nome, tipo di dispositivo esterno, azione da eseguire quando si collega un dispositivo esterno al computer e gravità del rapporto.

Fare clic su **Aggiungi** oppure su **Modifica** per gestire una regola. Fare clic su **Copia** per creare una nuova regola con le opzioni predefinite utilizzate per un'altra regola selezionata. Le stringhe XML visualizzate quando si seleziona una regola possono essere copiate negli Appunti in modo da essere utili agli amministratori di sistema per esportare/importare questi dati e utilizzarli, ad esempio in ESET Remote Administrator.

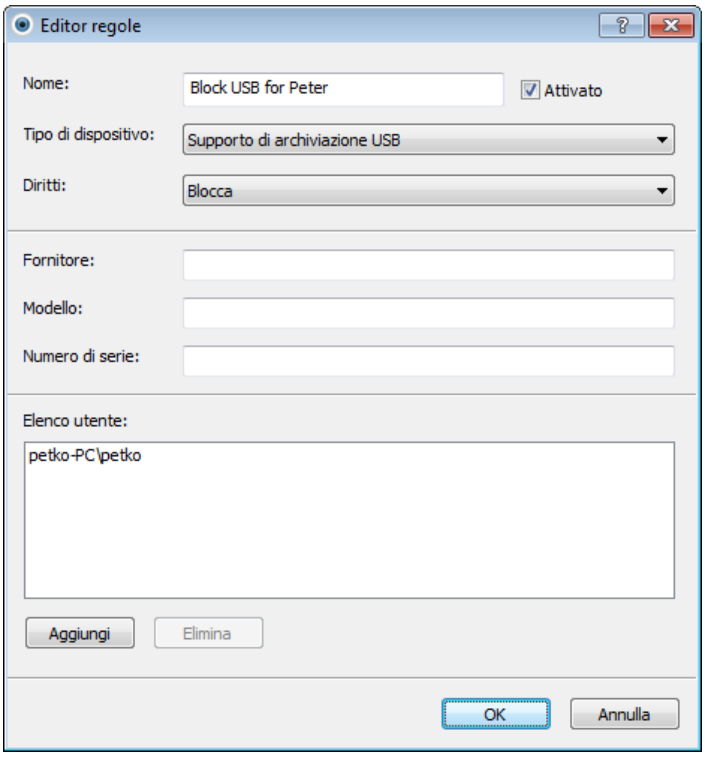
Premere CTRL e fare clic per selezionare più regole e applicare azioni a tutte le regole selezionate, ad esempio per eliminarle o spostarle in alto o in basso nell'elenco. Selezionare la casella di controllo **Attivata** per disattivare o attivare una regola. Questa opzione è utile se non si desidera eliminare definitivamente la regola in modo da poterla utilizzare in futuro.

Il controllo viene eseguito mediante regole che sono classificate in base al rispettivo ordine di priorità, a partire dalle regole con priorità più alta.

Fare clic con il pulsante destro del mouse su una regola per visualizzare il menu contestuale. Qui è possibile impostare il livello di dettaglio (gravità) delle voci di rapporto di una regola. Le voci del rapporto possono essere visualizzate nella finestra principale di ESET Endpoint Security in **Strumenti** > **File di rapporto**.

4.1.3.2 Aggiunta di regole controllo dispositivi

Una regola controllo dispositivi definisce l'azione che verrà intrapresa quando al computer viene collegato un dispositivo che soddisfa i criteri della regola.



Immettere una descrizione della regola nel campo **Nome** per consentire una migliore identificazione. Selezionare la casella di controllo accanto ad **Attivata** per disattivare o attivare questa regola. Questa opzione può essere utile se non si desidera eliminare definitivamente la regola.

Tipo di dispositivo

Scegliere il tipo di dispositivo esterno dal menu a discesa (USB/Bluetooth/FireWire/...). I tipi di dispositivi vengono ereditati dal sistema operativo e possono essere visualizzati in Gestione dispositivi del sistema, a condizione che un dispositivo sia collegato al computer. Il tipo di dispositivo **Supporto di archiviazione ottico** nel menu a discesa si riferisce all'archiviazione dei dati su un supporto leggibile a livello ottico (ad es. CD, DVD). I supporti di archiviazione includono dischi esterni o lettori convenzionali di schede di memoria collegati tramite USB o FireWire. Esempi di dispositivi di acquisizione immagini sono gli scanner o le fotocamere. I lettori di smart card includono lettori di smart card con un circuito integrato incorporato, ad esempio schede SIM o schede di autenticazione.

Diritti

È possibile negare o consentire l'accesso ai supporti non di archiviazione. Le regole dei supporti di archiviazione consentono invece di scegliere uno dei diritti seguenti:

- **Blocca** - L'accesso al supporto sarà bloccato.
- **Solo lettura** - Sul supporto sarà consentita solo la lettura.
- **Lettura/scrittura** - Sarà consentito l'accesso completo al supporto.

Tenere presente che non sono disponibili tutti i diritti (azioni) per tutti i tipi di dispositivi. Se se un supporto è disponibile spazio di archiviazione, saranno rese disponibili tutte le tre azioni. Per i supporti non di archiviazione, sono disponibili solo due azioni (ad esempio l'azione **Solo lettura** non è disponibile per Bluetooth. Ciò significa che il supporto può essere solo consentito o bloccato).

Altri parametri che possono essere utilizzati per ottimizzare le regole e personalizzarle in base ai dispositivi in uso. Tutti i parametri non fanno distinzione tra lettere maiuscole e minuscole:

- **Fornitore** - Filtraggio in base al nome o identificativo del fornitore.
- **Modello** - Nome specifico del dispositivo.
- **Numero di serie** - In genere a ogni dispositivo esterno è associato un numero di serie. Nel caso di CD/DVD, il numero di serie è associato al supporto specifico e non all'unità CD.

Nota: se le tre precedenti voci non sono specificate, in fase di ricerca della corrispondenza la regola ignorerà tali campi.

Suggerimento: Per trovare i parametri di un dispositivo, creare una regola di autorizzazione per il tipo appropriato di dispositivi, collegare il dispositivo al computer, quindi controllare le proprietà del dispositivo in Rapporto controllo dispositivi.

Le regole possono essere limitate a determinati utenti o gruppi di utenti aggiungendoli all'**Elenco utente**:

- **Aggiungi** - Visualizza la finestra di dialogo **Tipo di oggetto: Utenti o Gruppi** che consente di selezionare gli utenti desiderati.
- **Elimina** - Rimuove l'utente selezionato dal filtro.

4.1.4 Sistema anti-intrusione basato su host (HIPS)

Il **Sistema anti-intrusione basato su host** (HIPS) protegge il sistema da malware o attività indesiderate che tentano di compromettere la sicurezza del computer. L'HIPS utilizza un'analisi comportamentale avanzata unita alle capacità di rilevamento del filtraggio di rete per il monitoraggio dei processi in esecuzione, dei file e delle chiavi del Registro di sistema. L'HIPS è una funzione distinta dalla protezione file system in tempo reale e non è un firewall; esso monitora solo i processi eseguiti all'interno del sistema operativo.

L'HIPS è disponibile in **Configurazione avanzata** (F5) facendo clic su **Computer** > **HIPS**. Lo stato HIPS (attivato/disattivato) è mostrato nella finestra principale di ESET Endpoint Security, nel riquadro **Configurazione** a destra della sezione **Computer**.

Le impostazioni dell'HIPS sono disponibili in **Configurazione avanzata** (F5). Per accedere all'HIPS nella struttura Configurazione avanzata, fare clic su **Computer** > **HIPS**. Lo stato HIPS (attivato/disattivato) è visualizzato nella finestra principale di ESET Endpoint Security, nel riquadro **Configurazione** a destra della sezione Computer.

Attenzione: è consigliabile che le modifiche alle impostazioni HIPS siano apportate solo dagli utenti avanzati.

ESET Endpoint Security integra una tecnologia di Autoprotezione che impedisce a software dannoso di danneggiare o disattivare la protezione antivirus e antispyware, in modo da garantire costantemente la protezione del sistema. Le modifiche alle impostazioni **Attiva HIPS** e **Attiva l'Autoprotezione** avranno effetto solo dopo aver riavviato il sistema operativo Windows. Sarà necessario riavviare il computer anche se si disattiva l'intero sistema **HIPS**.

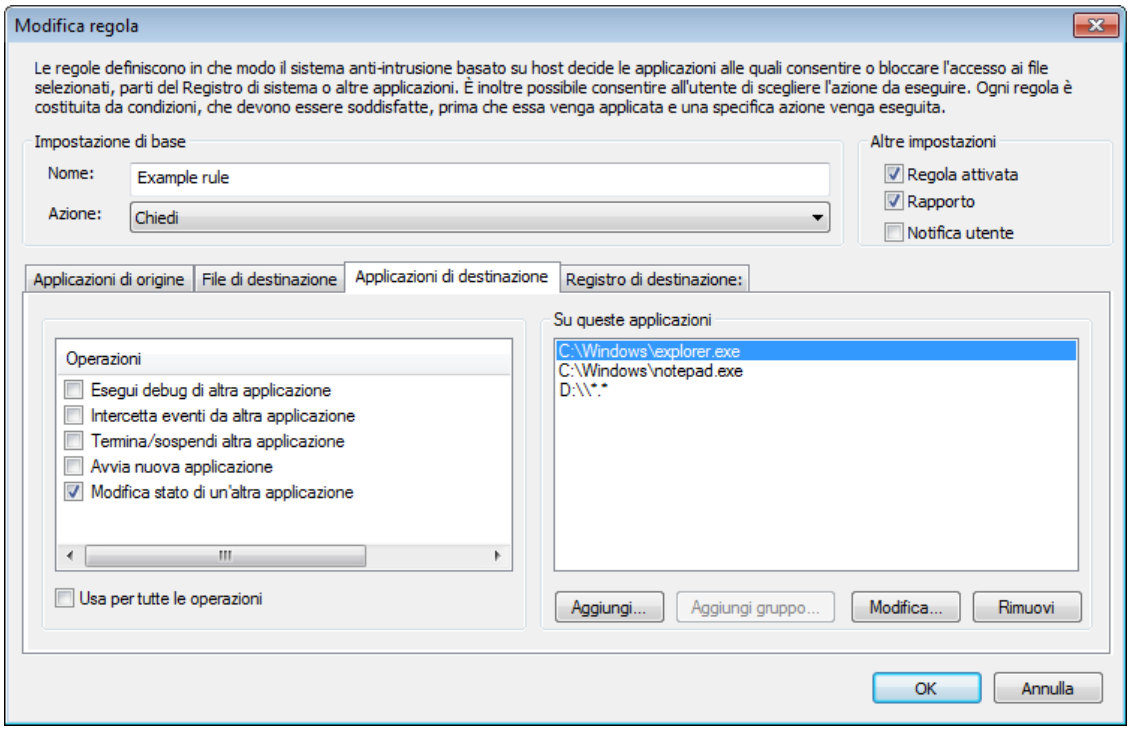
Il filtraggio può essere eseguito in uno delle quattro modalità:

- **Modalità automatica con regole** - Le operazioni sono attivate, ad eccezione delle regole predefinite che proteggono il sistema.
- **Modalità interattiva** - All'utente verrà chiesto di confermare le operazioni da eseguire.
- **Modalità basata su policy** - Le operazioni sono bloccate.
- **Modalità riconoscimento** - Le operazioni sono attivate e dopo ogni operazione viene creata una regola. Le regole create in questa modalità possono essere visualizzate nell'**Editor regole**, ma la loro priorità è inferiore rispetto alla priorità delle regole create manualmente o delle regole create nella modalità automatica. Dopo aver selezionato **Modalità riconoscimento**, l'opzione **Notifica scadenza modalità riconoscimento entro x giorni** diventa disponibile. Al termine di tale intervallo di tempo, la modalità riconoscimento viene nuovamente disattivata. Il periodo di tempo massimo è 14 giorni. Alla scadenza di tale intervallo di tempo, viene visualizzata una finestra popup in cui è possibile modificare le regole e selezionare una modalità di filtraggio differente.

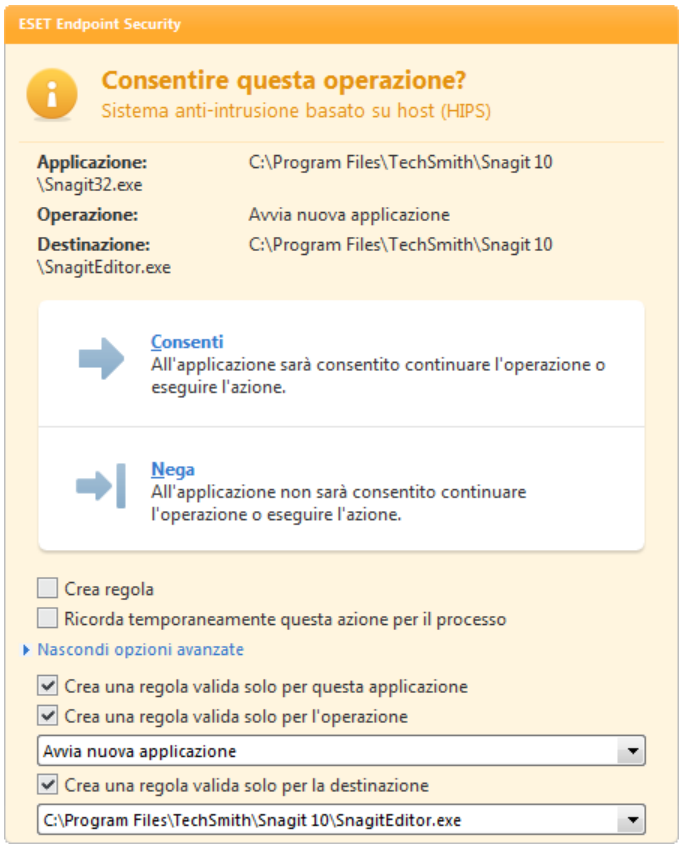
Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a regole simili alle regole usate dal Firewall. Fare clic su **Configura regole...** per aprire la finestra di gestione delle regole HIPS. In questa sezione è possibile selezionare, creare, modificare o eliminare regole.

Nell'esempio seguente viene spiegato come limitare il comportamento indesiderato delle applicazioni:

1. Denominare la regola e selezionare **Blocca** nel menu a discesa **Azione**.
2. Aprire la scheda **Applicazioni di destinazione**. Lasciare vuota la scheda **Applicazioni di origine** per applicare la nuova regola a tutte le applicazioni che tentano di eseguire una delle operazioni selezionate nell'elenco **Operazioni** sulle applicazioni nell'elenco **Su queste applicazioni**.
3. Selezionare **Modifica stato di un'altra applicazione** (tutte le operazioni sono descritte nella Guida del prodotto, premere il tasto F1 nella finestra che è uguale all'immagine seguente).
4. Aggiungere una o più applicazioni che si desidera proteggere.
5. Attivare l'opzione **Notifica utente** per visualizzare una notifica utente ogni volta che viene applicata la regola.
6. Fare clic su **OK** per salvare la nuova regola.


Modifica regola
Le regole definiscono in che modo il sistema anti-intrusione basato su host decide le applicazioni alle quali consentire o bloccare l'accesso ai file selezionati, parti del Registro di sistema o altre applicazioni. È inoltre possibile consentire all'utente di scegliere l'azione da eseguire. Ogni regola è costituita da condizioni, che devono essere soddisfatte, prima che essa venga applicata e una specifica azione venga eseguita.
Impostazione di base
Nome:
Example rule
Azione:
Chiedi
Altre impostazioni
Regola attivata
Rapporto
Notifica utente
Applicazioni di origine
File di destinazione
Applicazioni di destinazione
Registro di destinazione:
Operazioni
Esegui debug di altra applicazione
Intercetta eventi da altra applicazione
Termina/sospendi altra applicazione
Avvia nuova applicazione
Modifica stato di un'altra applicazione
Usa per tutte le operazioni
Su queste applicazioni
C:\Windows\explorer.exe
C:\Windows\notepad.exe
D:*.*
Aggiungi...
Aggiungi gruppo...
Modifica...
Rimuovi
OK
Annulla

Se l'azione predefinita è impostata su **Chiedi**, verrà sempre visualizzata una finestra di dialogo. In questa finestra l'utente può scegliere di eseguire l'azione **Nega** o **Consenti** l'operazione. Se l'utente non sceglie un'azione nell'intervallo di tempo previsto, viene selezionata una nuova azione in base alle regole.


ESET Endpoint Security
Consentire questa operazione?
Sistema anti-intrusione basato su host (HIPS)
Applicazione:
C:\Program Files\TechSmith\Snagit 10\Snagit32.exe
Operazione:
Avvia nuova applicazione
Destinazione:
C:\Program Files\TechSmith\Snagit 10\SnagitEditor.exe
Consenti
All'applicazione sarà consentito continuare l'operazione o eseguire l'azione.
Nega
All'applicazione non sarà consentito continuare l'operazione o eseguire l'azione.
Crea regola
Ricorda temporaneamente questa azione per il processo
Nascondi opzioni avanzate
Crea una regola valida solo per questa applicazione
Crea una regola valida solo per l'operazione
Avvia nuova applicazione
Crea una regola valida solo per la destinazione
C:\Program Files\TechSmith\Snagit 10\SnagitEditor.exe

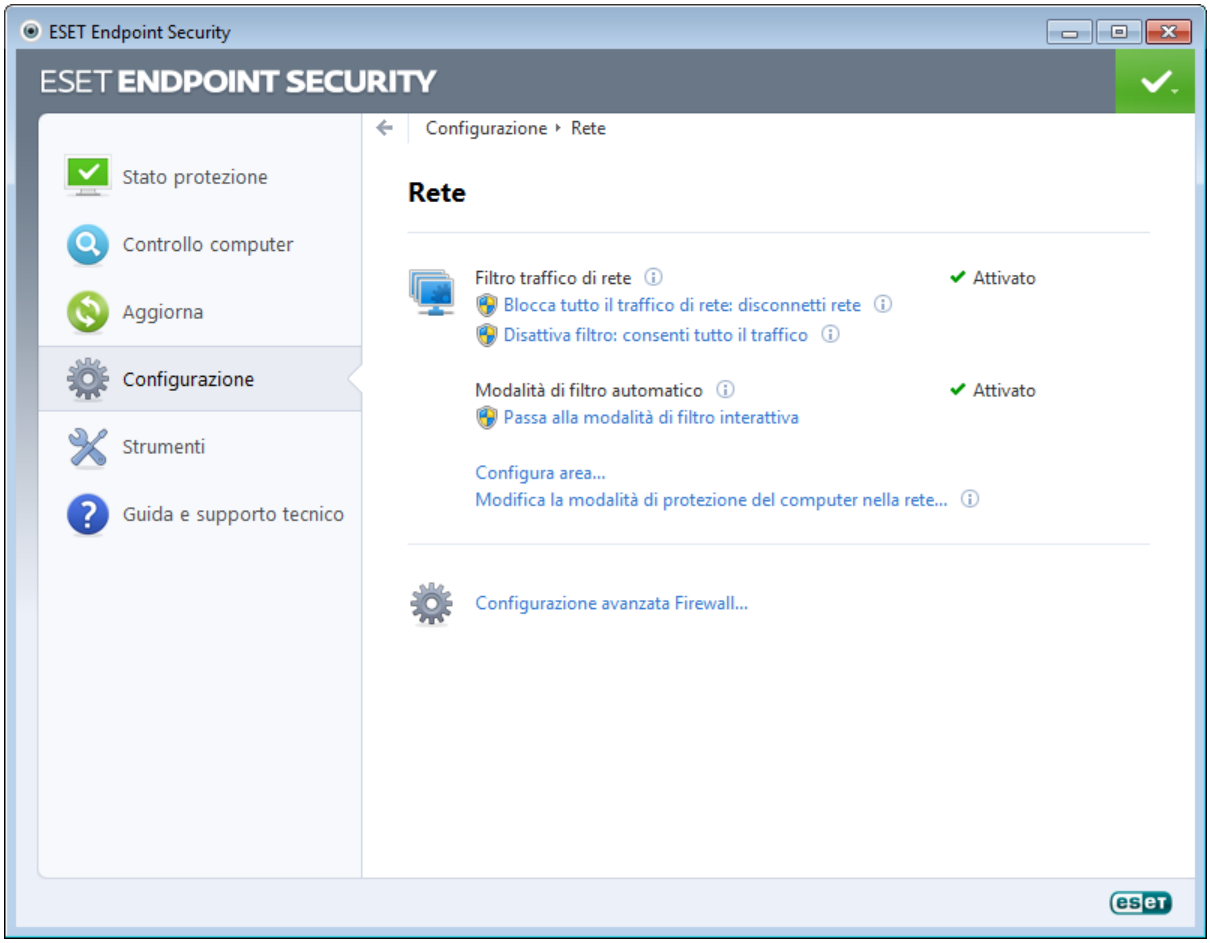
La finestra di dialogo consente di creare una regola in base a qualsiasi nuova azione rilevata dall'HIPS e di definire le condizioni in base alle quali consentire o negare tale azione. È possibile accedere alle impostazioni per i parametri esatti facendo clic su **Mostra opzioni**. Le regole create in questo modo sono considerate uguali alla regole create manualmente. Una regola creata da una finestra di dialogo può quindi essere meno specifica rispetto alla regola che ha attivato tale finestra di dialogo. Ciò significa che, dopo aver creato una tale regola, la stessa operazione può attivare la stessa finestra.

L'opzione **Ricorda temporaneamente questa azione per il processo** consente di utilizzare l'azione (**Consenti** / **Nega**) finché non verrà attuata una modifica delle regole o della modalità di filtraggio oppure un aggiornamento del modulo HIPS o un riavvio del sistema. In seguito ad una di queste tre azioni, le regole temporanee verranno eliminate.

4.2 Rete

Il Firewall personale controlla tutto il traffico di rete in entrata e in uscita dal sistema, consentendo o rifiutando singole connessioni di rete in base a specifiche regole di filtraggio. Offre protezione contro gli attacchi di computer remoti e consente di bloccare alcuni servizi. Offre inoltre protezione antivirus per i protocolli HTTP, POP3 e IMAP. Questa funzionalità rappresenta un elemento molto importante nella protezione del computer.

Le opzioni di configurazione del Firewall personale sono disponibili nel riquadro **Configurazione** facendo clic sul titolo **Rete**. Questa opzione consente di impostare la modalità di filtraggio, le regole e le impostazioni dettagliate. Da qui è inoltre possibile accedere alle impostazioni dettagliate del programma.



L'unica opzione disponibile per bloccare in modo completo tutto il traffico di rete è **Blocca tutto il traffico: disconnetti rete**. Tutte le altre comunicazione in entrata e in uscita saranno bloccate dal Firewall. Utilizzare questa opzione solo se si sospettano rischi di protezione critici che richiedono la disconnessione del sistema dalla rete.

L'opzione **Disattiva filtro: consenti tutto il traffico** esegue le funzioni opposte al blocco di tutto il traffico di rete. Se selezionata, tutte le opzioni di filtraggio del Firewall personale saranno disattivate e tutte le connessioni in ingresso e in uscita saranno consentite. L'effetto è pari alla mancanza di un firewall. Quando lo stato dell'opzione Filtro traffico di rete è **Blocco**, l'opzione **Passa alla modalità di filtraggio** consente di attivare il firewall.

Le opzioni seguenti sono disponibili quando la Modalità di filtro automatica è attivata:

- **Modalità di filtro automatica** - Per modificare la modalità di filtro, fare clic sull'opzione **Passa alla modalità di filtro interattiva**.
- **Configurazione area...** - Visualizza le opzioni di configurazione dell'area attendibile.

Le opzioni seguenti sono disponibili quando la Modalità di filtro interattiva è attivata:

- **Modalità di filtro interattiva** - Per modificare la modalità di filtraggio, fare clic sull'opzione**Passa alla modalità di filtro automatica** o **Passa alla modalità di filtro automatica con eccezioni** a seconda della modalità di filtraggio corrente.
- **Configura regole e aree...** - Consente di visualizzare la finestra **Configurazione area e regola** per definire le modalità di gestione delle comunicazioni di rete da parte del firewall.

Modifica la modalità di protezione del computer nella rete... - Consente di scegliere la modalità di protezione

massima o consentita.

Configurazione avanzata personal firewall... - Consente di accedere alle opzioni di impostazione avanzate del firewall.

4.2.1 Modalità di filtraggio

Per il Firewall ESET Endpoint Security sono disponibili cinque modalità di filtro. Le modalità di filtro sono disponibili in **Configurazione avanzata** (F5) facendo clic su **Rete** > **Firewall**. Il comportamento del firewall varia in base alla modalità selezionata. Le modalità di filtro influenzano inoltre il livello richiesto di interazione da parte dell'utente.

Il filtraggio può essere eseguito in uno delle cinque modalità:

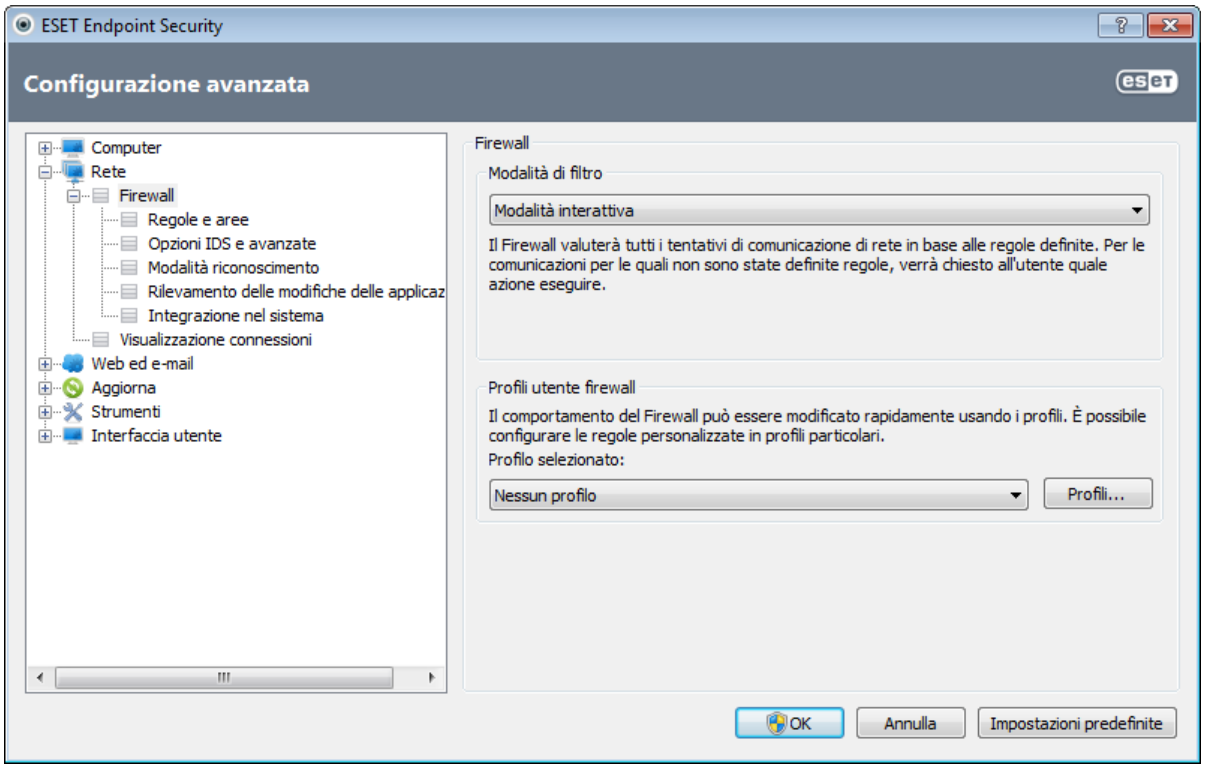
Modalità automatica - La modalità predefinita. È adatta agli utenti che preferiscono un utilizzo semplice e comodo del firewall senza che sia necessario definire regole. La modalità automatica consente tutto il traffico in uscita per il sistema e blocca tutte le nuove connessioni avviate sul lato rete.

Modalità automatica con eccezioni (regole definite dall'utente) - Oltre alla modalità automatica, è inoltre possibile aggiungere regole personalizzate definite dall'utente.

Modalità interattiva - Consente di creare una configurazione personalizzata per il Firewall personale. Quando viene rilevata una comunicazione per la quale non esiste alcuna regola applicabile, viene visualizzata una finestra di dialogo che segnala una connessione sconosciuta. La finestra di dialogo consente di accettare o rifiutare la comunicazione e la decisione può essere ricordata come nuova regola del Firewall personale. Se si decide di creare una nuova regola, tutte le connessioni future di questo tipo saranno consentite o bloccate in base a questa regola.

Modalità basata su criteri - Blocca tutte le connessioni non definite da una regola specifica che le consente. Questa modalità consente agli utenti esperti di definire regole che consentano solo connessioni sicure e desiderate. Tutte le altre connessioni non specificate saranno bloccate dal Firewall personale.

Modalità riconoscimento - Crea e salva automaticamente le regole. È inoltre ideale per la configurazione iniziale del Firewall personale. Non è richiesta alcuna interazione da parte dell'utente, poiché ESET Endpoint Security salva le regole in base a parametri predefiniti. La modalità riconoscimento non è una modalità protetta. Pertanto, è consigliabile utilizzarla solo fino a quando non siano state create tutte le regole richieste per le comunicazioni.

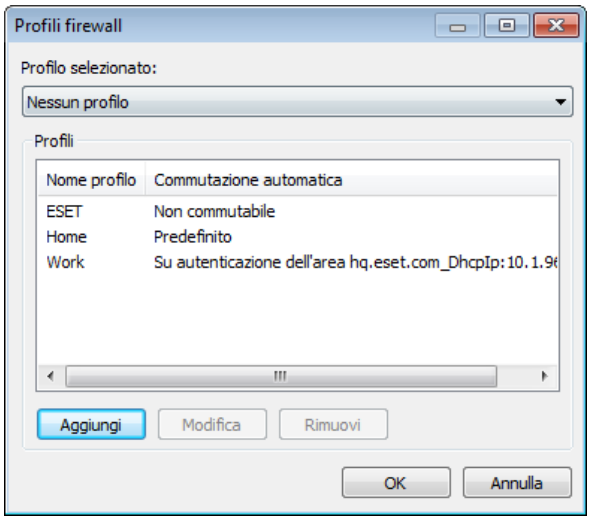


I profili sono uno strumento per controllare il comportamento del Firewall ESET Endpoint Security.

4.2.2 Profili firewall

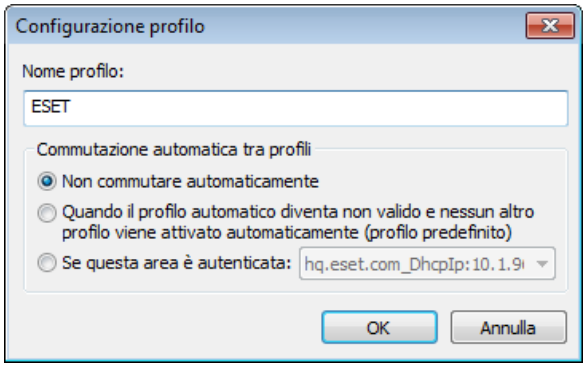
I profili possono essere utilizzati per controllare il comportamento del Firewall ESET Endpoint Security. Quando si crea o si modifica una regola del Firewall personale, è possibile assegnarla a un profilo specifico o applicarla a tutti i profili. Quando si seleziona un profilo, vengono applicate solo le regole globali (regole senza profilo specificato) e le regole assegnate a tale profilo. È possibile creare più profili con regole diverse per agevolare la modifica del comportamento del Firewall personale.

Fare clic sul pulsante **Profili...** (vedere la figura nella sezione Modalità di filtro) per aprire la finestra **Profili firewall** dove sono disponibili le opzioni **Aggiungi**, **Modifica** o **Rimuovi** profili. Tenere presente che per consentire le opzioni **Modifica** o **Rimuovi** profilo, il profilo non deve essere selezionato nel menu a discesa **Profilo selezionato**. Quando si aggiunge o si modifica un profilo, è anche possibile definire le condizioni per attivarlo.



Quando si crea un profilo, è possibile selezionare gli eventi che lo attiveranno. Sono disponibili le seguenti opzioni:

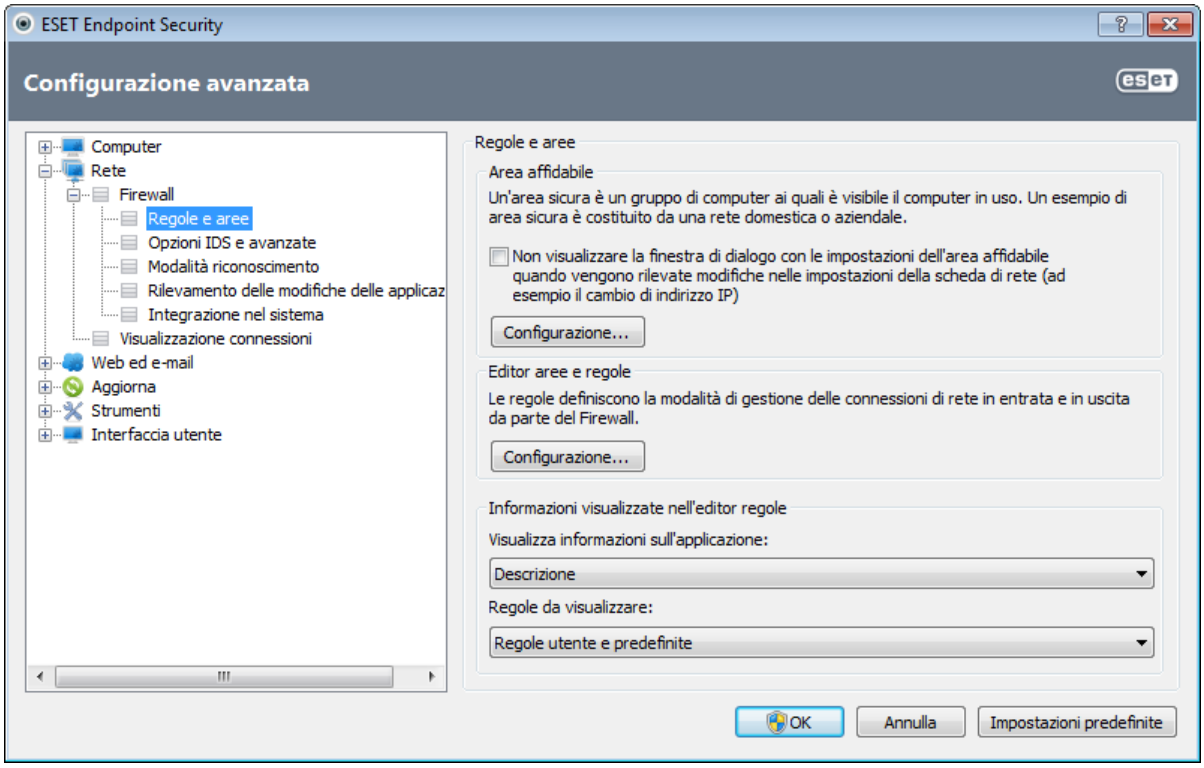
- **Non commutare automaticamente** - L'attivazione automatica è disattivata (il profilo deve essere attivato manualmente).
- **Quando il profilo automatico diventa non valido e nessun altro profilo viene attivato automaticamente (profilo predefinito)** - Quando il profilo automatico diventa non valido (il computer è collegato a una rete non attendibile, consultare la sezione Autenticazione di rete) e nessun altro profilo viene attivato al suo posto (il computer non è collegato ad altre reti attendibili), il Firewall personale passerà a questo profilo. Questa opzione consente di attivare un solo profilo.
- **Se questa area è autenticata** - Questo profilo sarà attivato quando viene autenticata l'area specificata (consultare la sezione Autenticazione di rete).



Quando il Firewall personale passa a un altro profilo, viene visualizzata una notifica nell'angolo in basso a destra, vicino all'orologio di sistema.

4.2.3 Configurazione e uso delle regole

Le regole rappresentano un insieme di condizioni utilizzate per testare tutte le connessioni di rete e tutte le azioni assegnate a queste condizioni. Nel caso in cui sia stabilita una connessione definita da una regola, nel Firewall personale è possibile stabilire l'azione da eseguire. Per accedere all'impostazione di filtraggio della regola, selezionare **Configurazione avanzata** (F5) > **Rete** > **Firewall** > **Regole e aree**.


ESET Endpoint Security
Configurazione avanzata
Computer
Rete
Firewall
Regole e aree
Opzioni IDS e avanzate
Modalità riconoscimento
Rilevamento delle modifiche delle applicaz
Integrazione nel sistema
Visualizzazione connessioni
Web ed e-mail
Aggiorna
Strumenti
Interfaccia utente
Regole e aree
Area affidabile
Un'area sicura è un gruppo di computer ai quali è visibile il computer in uso. Un esempio di area sicura è costituito da una rete domestica o aziendale.
Non visualizzare la finestra di dialogo con le impostazioni dell'area affidabile quando vengono rilevate modifiche nelle impostazioni della scheda di rete (ad esempio il cambio di indirizzo IP)
Configurazione...
Editor aree e regole
Le regole definiscono la modalità di gestione delle connessioni di rete in entrata e in uscita da parte del Firewall.
Configurazione...
Informazioni visualizzate nell'editor regole
Visualizza informazioni sull'applicazione:
Descrizione
Regole da visualizzare:
Regole utente e predefinite
OK
Annulla
Impostazioni predefinite

Fare clic sul pulsante **Configurazione...** nella sezione **Area affidabile** per visualizzare la finestra di dialogo di configurazione dell'area affidabile. L'opzione **Non visualizzare con le impostazioni Area affidabile...** consente all'utente di disattivare la visualizzazione automatica della finestra di configurazione dell'area affidabile ogni volta che viene rilevata la presenza di una nuova subnet. Viene utilizzata automaticamente la configurazione dell'area attualmente specificata.

NOTA: se il Firewall personale è impostato sulla **Modalità automatica**, queste impostazioni non saranno disponibili.

Fare clic sul pulsante Configura... nella sezione **Editor aree e regole** per visualizzare la finestra **Configurazione area e regola** contenente una panoramica delle regole o delle aree (in base alla scheda correntemente selezionata). La finestra è suddivisa in due sezioni. Nella sezione superiore è visualizzato un elenco sintetico di tutte le regole. Nella sezione inferiore sono visualizzati dettagli sulla regola selezionata nella sezione superiore. Nella parte inferiore della finestra i pulsanti **Nuova**, **Modifica** ed **Elimina (CANC)** consentono di configurare le regole.

Le connessioni possono essere suddivise in connessioni in entrata e in uscita. Le connessioni in entrata vengono avviate da un computer remoto che tenta di stabilire una connessione con il sistema locale. Le connessioni in uscita funzionano in senso opposto: il sistema locale tenta di stabilire la connessione con un computer remoto.

Quando viene rilevata una nuova comunicazione sconosciuta, è necessario considerare con attenzione se accettarla o rifiutarla. Le connessioni non desiderate, non sicure o sconosciute costituiscono un rischio per la protezione del sistema. Nel caso in cui venga stabilita una connessione di questo tipo, è consigliabile prestare particolare attenzione al computer remoto e all'applicazione che tenta di connettersi al computer. Molte infiltrazioni cercano di ottenere e inviare dati privati o scaricare altre applicazioni dannose sulle workstation host. Il Firewall personale consente di rilevare e terminare queste connessioni.

Visualizza informazioni sull'applicazione consente di definire le applicazioni che verranno visualizzate nell'elenco di regole. Sono disponibili le seguenti opzioni:

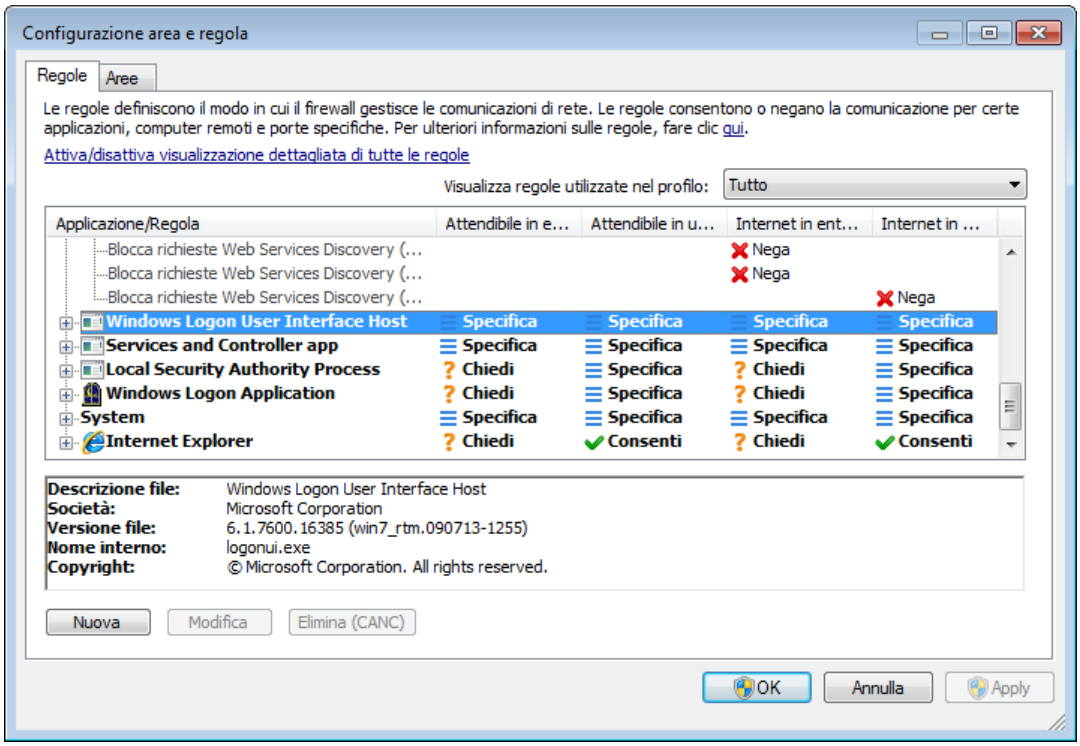
- **Percorso completo** - Percorso completo dell'eseguibile dell'applicazione.
- **Descrizione** - Descrizione dell'applicazione.
- **Nome** – Nome dell'eseguibile dell'applicazione.

Selezionare il tipo di regole che saranno visualizzate nell'elenco **Regole da visualizzare**:

- **Solo regole definite dall'utente** - Consente di visualizzare solo le regole create dall'utente.
- **Regole utente e predefinite** - Consente di visualizzare tutte le regole definite dall'utente e le regole predefinite.
- **Tutte le regole (incluso sistema)** - Vengono visualizzate tutte le regole.

4.2.3.1 Configurazione delle regole

La Configurazione delle regole consente di visualizzare tutte le regole applicate al traffico generato dalle singole applicazioni all'interno delle aree attendibili e di Internet. Per impostazione predefinita, le regole vengono aggiunte automaticamente in base alle reazioni dell'utente a una nuova comunicazione. Per visualizzare ulteriori informazioni su un'applicazione nella parte inferiore di questa finestra, fare clic sul nome dell'applicazione.



All'inizio di ogni riga corrispondente a una regola, è presente un pulsante che consente di espandere/comprimere (+/-) le informazioni. Fare clic sul nome dell'applicazione nella colonna **Applicazione/Regola** per visualizzare le informazioni sulla regola nella parte inferiore della finestra. È possibile utilizzare il menu contestuale per modificare la modalità di visualizzazione. È inoltre possibile utilizzare il menu contestuale per aggiungere, modificare ed eliminare le regole.

Ingresso/uscita area sicura - Azioni correlate alle comunicazioni in entrata o in uscita all'interno dell'area affidabile.

Ingresso/uscita Internet - Azioni correlate alle comunicazioni in entrata o in uscita in relazione alla connessione Internet.

Per ciascun tipo (direzione) di comunicazione, è possibile selezionare le azioni seguenti:

- ✔ **Consenti** - Per consentire le comunicazioni.
- ? **Chiedi** - Ogni volta che deve essere stabilita una comunicazione, all'utente verrà richiesto di consentire oppure negare la comunicazione.
- ✘ **Nega** - Per negare le comunicazioni.
- ≡ **Specifica** - Non può essere classificata rispetto ad altre azioni. Se ad esempio un indirizzo IP o una porta sono consentite tramite il Firewall, non può essere classificata con certezza, indipendentemente dal fatto che le comunicazioni in entrata e in uscita di un'applicazione correlata siano consentite.

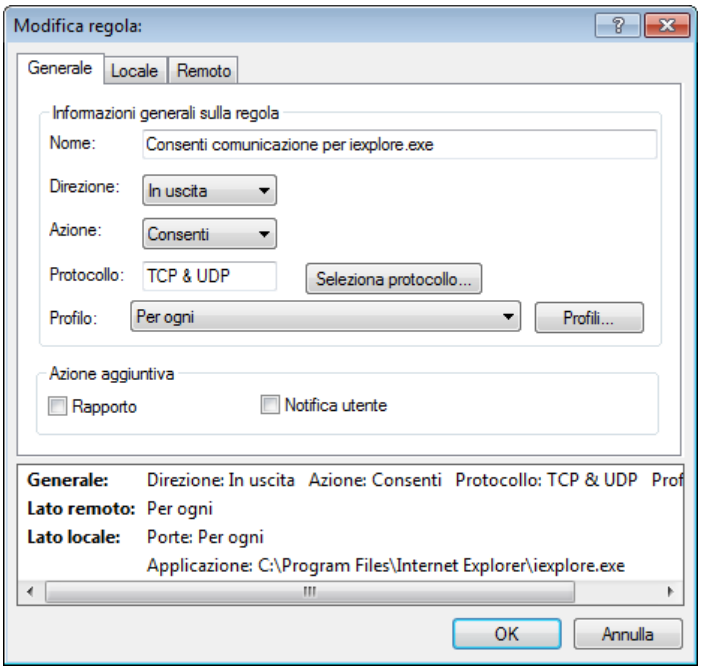
Durante l'installazione di una nuova applicazione con accesso alla rete o in caso di modifica di una connessione esistente (lato remoto, numero di porta e così via), è necessario creare una nuova regola. Per modificare una regola esistente, verificare che la scheda **Regole** sia selezionata, quindi fare clic sul pulsante **Modifica**.

4.2.3.2 Modifica delle regole

La modifica è necessaria ogni volta che uno dei parametri monitorati viene cambiato. In questo caso, la regola non soddisfa le condizioni e non è possibile applicare l'azione specificata. Se i parametri sono stati modificati, la connessione può essere rifiutata, causando eventuali problemi di funzionamento dell'applicazione in uso. Un esempio è la modifica di un indirizzo di rete o di un numero di porta per il lato remoto.

La parte superiore della finestra contiene tre schede:

- **Generale** - Specificare un nome per la regola, la direzione della connessione, l'azione, il protocollo e il profilo a cui si applicherà la regola.
- **Locale** - In questa scheda sono visualizzate informazioni sul lato locale della connessione, compreso il numero della porta locale o l'intervallo di porte e il nome dell'applicazione coinvolta nella comunicazione.
- **Remoto** - Questa scheda contiene informazioni sulla porta remota (intervallo porte). Consente inoltre di definire un elenco di indirizzi IP remoti o aree per una specifica regola.



Protocollo indica il protocollo di trasferimento utilizzato per la regola. Fare clic su **Seleziona protocollo...** per aprire la finestra Selezione protocollo.

Per impostazione predefinita, tutte le regole sono attivate **Per ogni** profilo. In alternativa, selezionare un profilo firewall personalizzato tramite il pulsante **Profili...**.

Se si seleziona **Rapporto**, l'attività correlata alla regola verrà memorizzata in un registro. L'opzione **Notifica utente** consente di visualizzare una notifica quando viene applicata la regola.

La casella Informazioni contiene un riepilogo della regola e viene visualizzata nella parte inferiore di tutte e tre le schede. Se si seleziona la regola nella finestra principale è possibile visualizzare le stesse informazioni (**Strumenti** > **Connessioni di rete**. Fare clic con il pulsante destro del mouse sulla regola e attivare l'opzione **Mostra dettagli** (consultare il capitolo Connessioni di rete)).

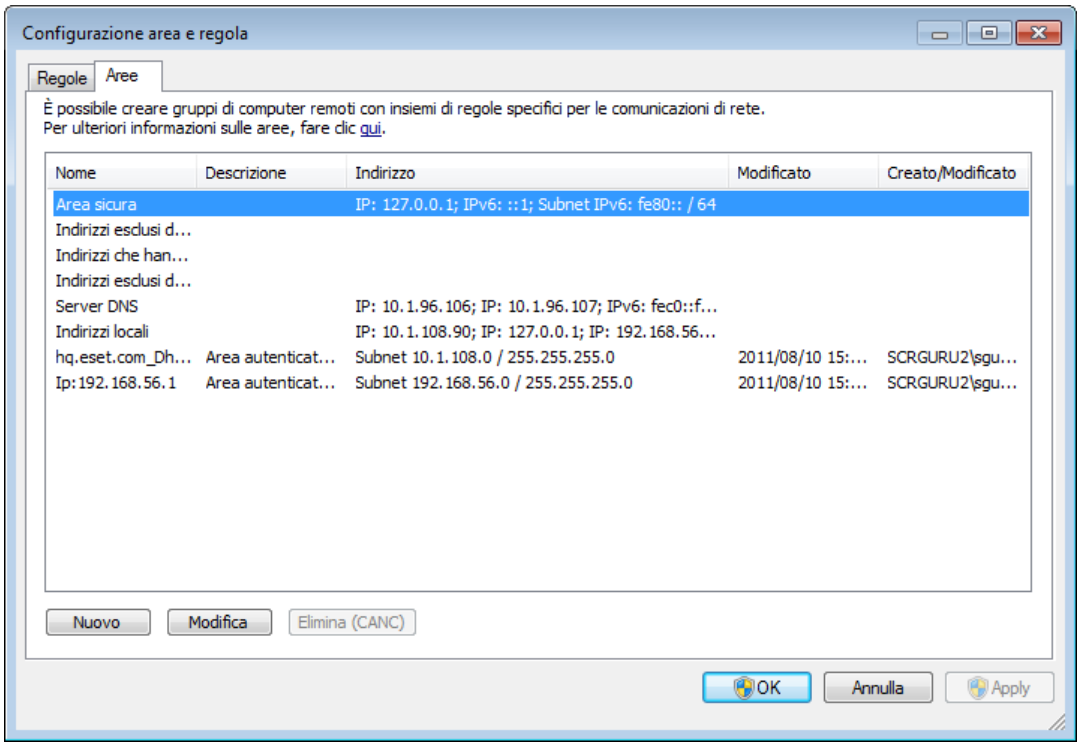
Quando si crea una nuova regola, è necessario immettere il relativo nome nel campo **Nome**. Selezionare la direzione alla quale si applica la regola nel menu a discesa **Direzione**. Impostare l'azione da eseguire quando una comunicazione soddisfa la regola nel menu a discesa **Azione**.

Un esempio di aggiunta di una nuova regola consiste nel consentire al browser Internet di accedere alla rete. In questo caso è consigliabile attenersi alla seguente procedura:

- Nella scheda **Generale**, attivare le comunicazioni in uscita mediante il protocollo TCP e UDP.
- Aggiungere il processo che rappresenta l'applicazione browser (per Internet Explorer è iexplore.exe) nella scheda **Locale**.
- Nella scheda **Remoto**, attivare il numero di porta 80 solo se si desidera consentire attività standard del browser Internet.

4.2.4 Configurazione aree

Nella finestra **Configurazione area** è possibile specificare il nome dell'area, la descrizione, l'elenco indirizzi di rete e l'autenticazione area (consultare Autenticazione area - Configurazione client).



Un'area rappresenta una raccolta di indirizzi di rete che creano un solo gruppo logico. A ogni indirizzo di un determinato gruppo sono assegnate regole simili definite centralmente per l'intero gruppo. Un esempio di gruppo di questo tipo è costituito dall'**Area affidabile**. L'Area affidabile rappresenta un gruppo di indirizzi di rete considerati completamente attendibili dall'utente e che non vengono in alcun modo bloccati dal Firewall personale.

È possibile configurare queste aree mediante la scheda **Aree** nella finestra **Configurazione area e regola**, utilizzando il pulsante **Modifica**. Immettere un **Nome** per l'area e una **Descrizione**, quindi aggiungere un indirizzo IP remoto selezionando il pulsante **Aggiungi indirizzo IPv4/IPv6**.

4.2.4.1 Autenticazione di rete

Per i computer portatili è consigliabile verificare l'affidabilità della rete alla quale si sta tentando di connettersi. L'Area affidabile è identificata dall'indirizzo IP locale della scheda di rete. Spesso i computer portatili accedono alle reti con indirizzi IP simili alla rete attendibile. Se le impostazioni dell'area affidabile non vengono commutate manualmente su **Massima protezione**, il firewall personale continuerà a utilizzare la modalità **Consenti condivisione**.

Per evitare questo tipo di situazione, è consigliabile utilizzare l'autenticazione dell'area.

4.2.4.1.1 Autenticazione area - Configurazione client

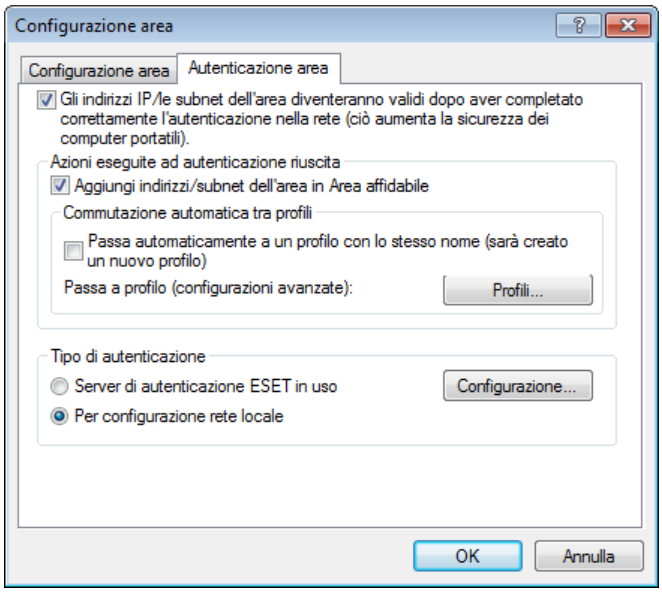
Nella finestra **Configurazione area e regola**, fare clic sulla scheda **Aree** e creare una nuova area utilizzando il nome dell'area autenticata dal server. Quindi fare clic su **Aggiungi indirizzo IPv4** e selezionare l'opzione **Subnet** per aggiungere una maschera subnet contenente il server di autenticazione.

Fare clic sulla scheda **Autenticazione area**. Ogni area può essere impostata in modo che si autenticata sul server. L'area (e il rispettivo indirizzo IP e subnet) sarà valida dopo essere stata correttamente autenticata. Ad esempio, azioni quali il passaggio a un profilo firewall e l'aggiunta di un indirizzo/subnet dell'area all'Area affidabile saranno eseguite solo dopo che l'autenticazione è stata eseguita correttamente.

Selezionare l'opzione **Gli indirizzi IP/le subnet dell'area diventeranno validi...** per non rendere valida un'area nel caso in cui l'autenticazione non venga eseguita correttamente. Per selezionare un profilo di Firewall personale da attivare dopo un'autenticazione area riuscita, fare clic sul pulsante **Profili...**.

Selezionando l'opzione **Aggiungi indirizzi/subnet dell'area in Area affidabile**, gli indirizzi/le subnet dell'area saranno aggiunti all'area affidabile dopo un'autenticazione riuscita (opzione consigliata). Se l'autenticazione non è riuscita, gli indirizzi non saranno aggiunti all'area affidabile. Se è attiva l'opzione **Passa automaticamente a un profilo con lo stesso nome (sarà creato un nuovo profilo)**, il nuovo profilo sarà creato dopo l'autenticazione riuscita. Fare clic sul

pulsante **Profili...** per visualizzare la finestra Profili firewall.


Configurazione area
Configurazione area
Autenticazione area
Gli indirizzi IP/le subnet dell'area diventeranno validi dopo aver completato correttamente l'autenticazione nella rete (ciò aumenta la sicurezza dei computer portatili).
Azioni eseguite ad autenticazione riuscita
Aggiungi indirizzi/subnet dell'area in Area affidabile
Commutazione automatica tra profili
Passa automaticamente a un profilo con lo stesso nome (sarà creato un nuovo profilo)
Passa a profilo (configurazioni avanzate):
Profili...
Tipo di autenticazione
Server di autenticazione ESET in uso
Configurazione...
Per configurazione rete locale
OK
Annulla

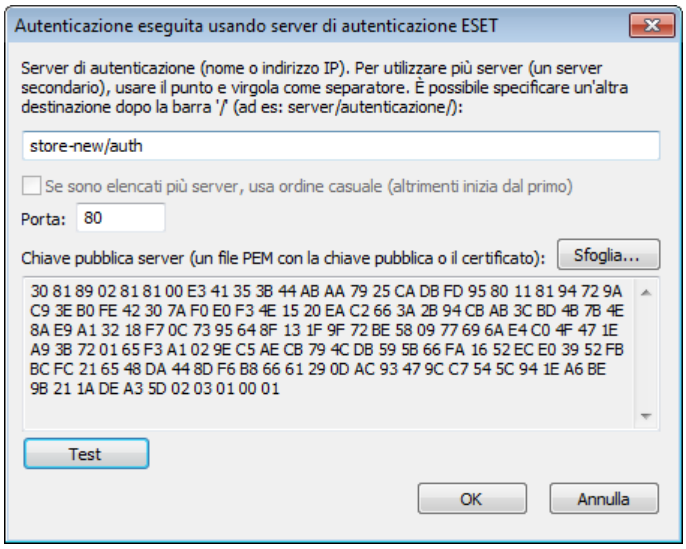
Sono disponibili due tipi di autenticazione:

1) Server di autenticazione ESET in uso

L'Autenticazione area ricerca un server specifico nella rete e utilizza la crittografia asimmetrica (RSA) per autenticare il server. La procedura di autenticazione viene ripetuta per ciascuna rete al quale il computer si connette. Fare clic su **Configurazione...** e specificare un nome del server, una porta di ascolto server e una chiave pubblica che corrisponde alla chiave privata server (consultare la sezione Autenticazione area - Configurazione server). Il nome del server può essere immesso sotto forma di indirizzo IP, DNS o nome NetBios. Il nome del server può essere seguito da un percorso che specifica la posizione della chiave sul server (ad esempio, server_name_/directory1/directory2/authentication). Immettere più server, separati da punti e vergola, affinché funzionino come server alternativi qualora il primo non fosse disponibile.

La chiave pubblica può essere un file dei tipi seguenti:

- Chiave pubblica crittografata PEM (.pem)
  Questa chiave può essere generata usando il server di autenticazione ESET (consultare la sezione Autenticazione area - Configurazione server).
- Chiave pubblica crittografata
- Certificato di chiave pubblica (.crt)


Autenticazione eseguita usando server di autenticazione ESET
Server di autenticazione (nome o indirizzo IP). Per utilizzare più server (un server secondario), usare il punto e virgola come separatore. È possibile specificare un'altra destinazione dopo la barra '/' (ad es: server/autenticazione/):
store-new/auth
Se sono elencati più server, usa ordine casuale (altrimenti inizia dal primo)
Porta: 80
Chiave pubblica server (un file PEM con la chiave pubblica o il certificato):
Sfoglia...
30 81 89 02 81 81 00 E3 41 35 3B 44 AB AA 79 25 CA DB FD 95 80 11 81 94 72 9A C9 3E B0 FE 42 30 7A F0 E0 F3 4E 15 20 EA C2 66 3A 2B 94 CB AB 3C BD 4B 7B 4E 8A E9 A1 32 18 F7 0C 73 95 64 8F 13 1F 9F 72 BE 58 09 77 69 6A E4 C0 4F 47 1E A9 3B 72 01 65 F3 A1 02 9E C5 AE CB 79 4C DB 59 5B 66 FA 16 52 EC E0 39 52 FB BC FC 21 65 48 DA 44 8D F6 B8 66 61 29 0D AC 93 47 9C C7 54 5C 94 1E A6 BE 9B 21 1A DE A3 5D 02 03 01 00 01
Test
OK
Annulla

Per testare le impostazioni, fare clic sul pulsante **Test**. Se l'autenticazione è riuscita, viene visualizzato il messaggio Autenticazione server riuscita. Se l'autenticazione non è configurata correttamente, viene visualizzato uno dei seguenti messaggi di errore:

Autenticazione server non riuscita. Tempo massimo per autenticazione scaduto.
Il server di autenticazione non è accessibile. Controllare il nome server/l'indirizzo IP e/o verificare le impostazioni del

firewall personale del client, nonché la sezione del server.

Si è verificato un errore durante la comunicazione con il server.
Il server di autenticazione non è in funzione. Avviare il servizio del server di autenticazione (consultare la sezione Autenticazione area - Configurazione server).

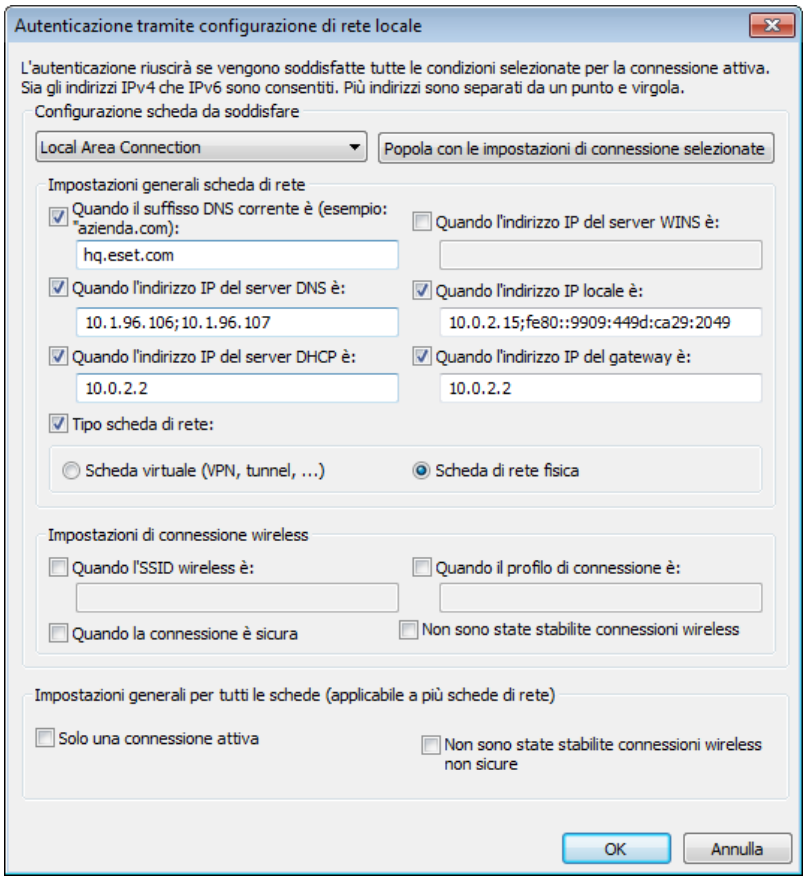
Il nome dell'area di autenticazione non corrisponde all'area del server.
Il nome dell'area configurato non corrisponde all'area del server di autenticazione. Controllare entrambe le aree e accertarsi che i nomi siano identici.

Autenticazione server non riuscita. Impossibile trovare l'indirizzo del server nell'elenco di indirizzi per l'area indicata.
L'indirizzo IP del computer che esegue il server di autenticazione non rientra nell'intervallo di indirizzi IP definito della configurazione area corrente.

Autenticazione server non riuscita. Probabilmente è stata inserita una chiave pubblica non valida.
Verificare che la chiave pubblica specificata corrisponda alla chiave privata server. Verificare inoltre che il file della chiave pubblica non sia corrotto.

2) Per configurazione rete locale

L'autenticazione viene eseguita in base ai parametri di una scheda di rete locale. Un'area è autenticata se tutti i parametri selezionati per la connessione attiva sono validi.


Autenticazione tramite configurazione di rete locale
L'autenticazione riuscirà se vengono soddisfatte tutte le condizioni selezionate per la connessione attiva.
Sia gli indirizzi IPv4 che IPv6 sono consentiti. Più indirizzi sono separati da un punto e virgola.
Configurazione scheda da soddisfare
Local Area Connection
Popola con le impostazioni di connessione selezionate
Impostazioni generali scheda di rete
Quando il suffisso DNS corrente è (esempio: "azienda.com):
hq.eset.com
Quando l'indirizzo IP del server WINS è:
Quando l'indirizzo IP del server DNS è:
10.1.96.106;10.1.96.107
Quando l'indirizzo IP locale è:
10.0.2.15;fe80::9909:449d:ca29:2049
Quando l'indirizzo IP del server DHCP è:
10.0.2.2
Quando l'indirizzo IP del gateway è:
10.0.2.2
Tipo scheda di rete:
Scheda virtuale (VPN, tunnel, ...)
Scheda di rete fisica
Impostazioni di connessione wireless
Quando l'SSID wireless è:
Quando il profilo di connessione è:
Quando la connessione è sicura
Non sono state stabilite connessioni wireless
Impostazioni generali per tutti le schede (applicabile a più schede di rete)
Solo una connessione attiva
Non sono state stabilite connessioni wireless non sicure
OK
Annulla

4.2.4.1.2 Autenticazione area - Configurazione server

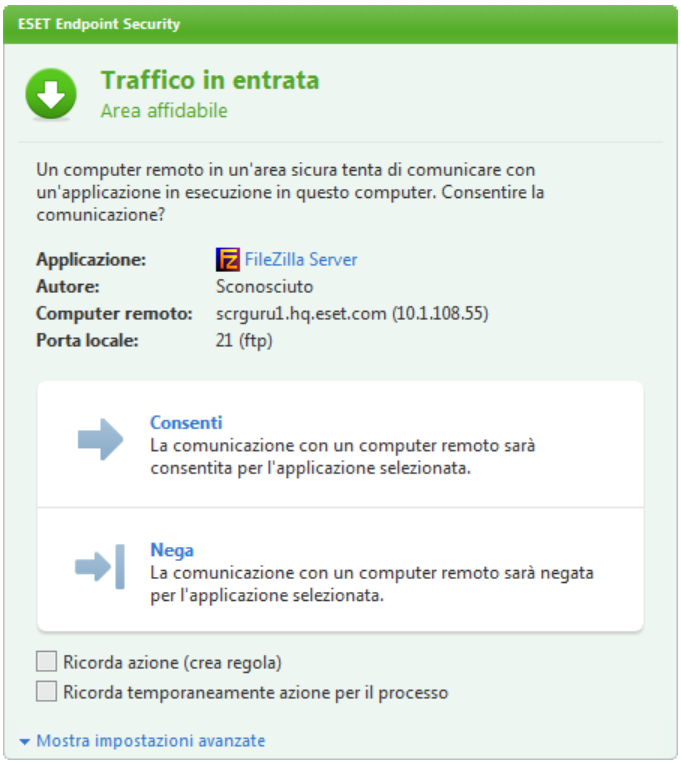
Il processo di autenticazione può essere eseguito da qualsiasi computer/server collegato alla rete da autenticare. L'applicazione Server di autenticazione ESET deve essere installata su un computer/server sempre accessibile per l'autenticazione ogniqualvolta un client tenti di collegarsi alla rete. Il file d'installazione per l'applicazione Server di autenticazione ESET è disponibile per il download sul sito Web ESET.

Dopo aver installato l'applicazione Server di autenticazione ESET, verrà visualizzata una finestra di dialogo (è possibile accedere all'applicazione da **Start** > **Programmi** > **ESET** > **Server di autenticazione ESET**).

Per configurare il server di autenticazione, immettere il nome dell'area di autenticazione, la porta di ascolto del server (l'impostazione predefinita è 80) e il percorso di archiviazione delle chiavi pubblica e privata. Generare quindi le chiavi pubblica e privata che saranno utilizzate nel processo di autenticazione. La chiave privata rimarrà sul server, mentre quella pubblica deve essere importata sul lato client nella sezione Autenticazione area durante la configurazione di un'area nell'impostazione del firewall.

4.2.5 Stabilire la connessione - rilevamento

Il Firewall personale rileva tutte le connessioni di rete non appena vengono create. La modalità di firewall attivo determina le azioni eseguite per la nuova regola. Se è attivata la **Modalità automatica** o la **Modalità basata su policy** , il Firewall personale eseguirà azioni predefinite senza alcun intervento da parte dell'utente. In Modalità interattiva viene invece visualizzata una finestra informativa che riporta il rilevamento di una nuova connessione di rete, con informazioni dettagliate sulla connessione. È possibile scegliere se consentire o rifiutare la connessione (bloccarla). Se si consente ripetutamente la stessa connessione nella finestra di dialogo, è consigliabile creare una nuova regola per tale connessione. Per eseguire questa operazione, selezionare l'opzione **Ricorda azione (crea regola)** e salvare l'azione come nuova regola per il Firewall personale. Se il firewall riconosce la stessa connessione in futuro, applicherà la regola esistente senza richiedere l'intervento da parte dell'utente.


ESET Endpoint Security
Traffico in entrata
Area affidabile
Un computer remoto in un'area sicura tenta di comunicare con un'applicazione in esecuzione in questo computer. Consentire la comunicazione?
Applicazione: FileZilla Server
Autore: Sconosciuto
Computer remoto: scrguru1.hq.eset.com (10.1.108.55)
Porta locale: 21 (ftp)
Consenti
La comunicazione con un computer remoto sarà consentita per l'applicazione selezionata.
Nega
La comunicazione con un computer remoto sarà negata per l'applicazione selezionata.
Ricorda azione (crea regola)
Ricorda temporaneamente azione per il processo
Mostra impostazioni avanzate

Prestare la massima attenzione durante la creazione di nuove regole e consentire solo le connessioni delle quali si è certi. Se si consentono tutte le connessioni, il Firewall personale non potrà svolgere la funzione per la quale è stato installato. Sono riportati di seguito importanti parametri per le connessioni:

- **Lato remoto** - Consentire la connessione solo a indirizzi affidabili e noti.
- **Applicazione locale** - Non è consigliabile consentire la connessione di applicazioni e processi sconosciuti.
- **Numero porta** - Consentire la comunicazione sulle porte comuni (ad esempio il traffico Web sulla porta 80) in normali circostanze.

Per poter proliferare, le infiltrazioni utilizzano spesso la connessione a Internet e connessioni nascoste per infettare sistemi remoti. Se le regole sono configurate correttamente, un firewall personale diventa uno strumento utile per la protezione contro numerosi attacchi di codice dannoso.

4.2.6 Registrazione

Il Firewall ESET Endpoint Security salva tutti gli eventi importanti in un file di rapporto, che può essere visualizzato direttamente dal menu principale. Scegliere **Strumenti** > **File di rapporto**, quindi selezionare**Rapporto del Firewall ESET** dal menu a discesa **Rapporto**.

I file di rapporto sono uno strumento importante per il rilevamento di errori e per rivelare intrusioni nel sistema. I rapporti del Firewall ESET contengono le informazioni seguenti:

- Data e ora dell'evento
- Nome dell'evento
- Origine
- Indirizzo della rete di destinazione
- Protocollo di comunicazione di rete
- Regola applicata o nome del worm, se identificato
- Applicazione coinvolta
- Utente

Un'attenta analisi di questi dati può essere utile per rilevare i tentativi di violare la protezione del sistema. Molti altri fattori indicano potenziali rischi per la protezione e consentono di ridurre al minimo il relativo impatto: connessioni troppo frequenti da posizioni sconosciute, tentativi ripetuti di stabilire connessioni, comunicazione da parte di applicazioni sconosciute o utilizzo di numeri di porte insoliti.

4.2.7 Integrazione nel sistema

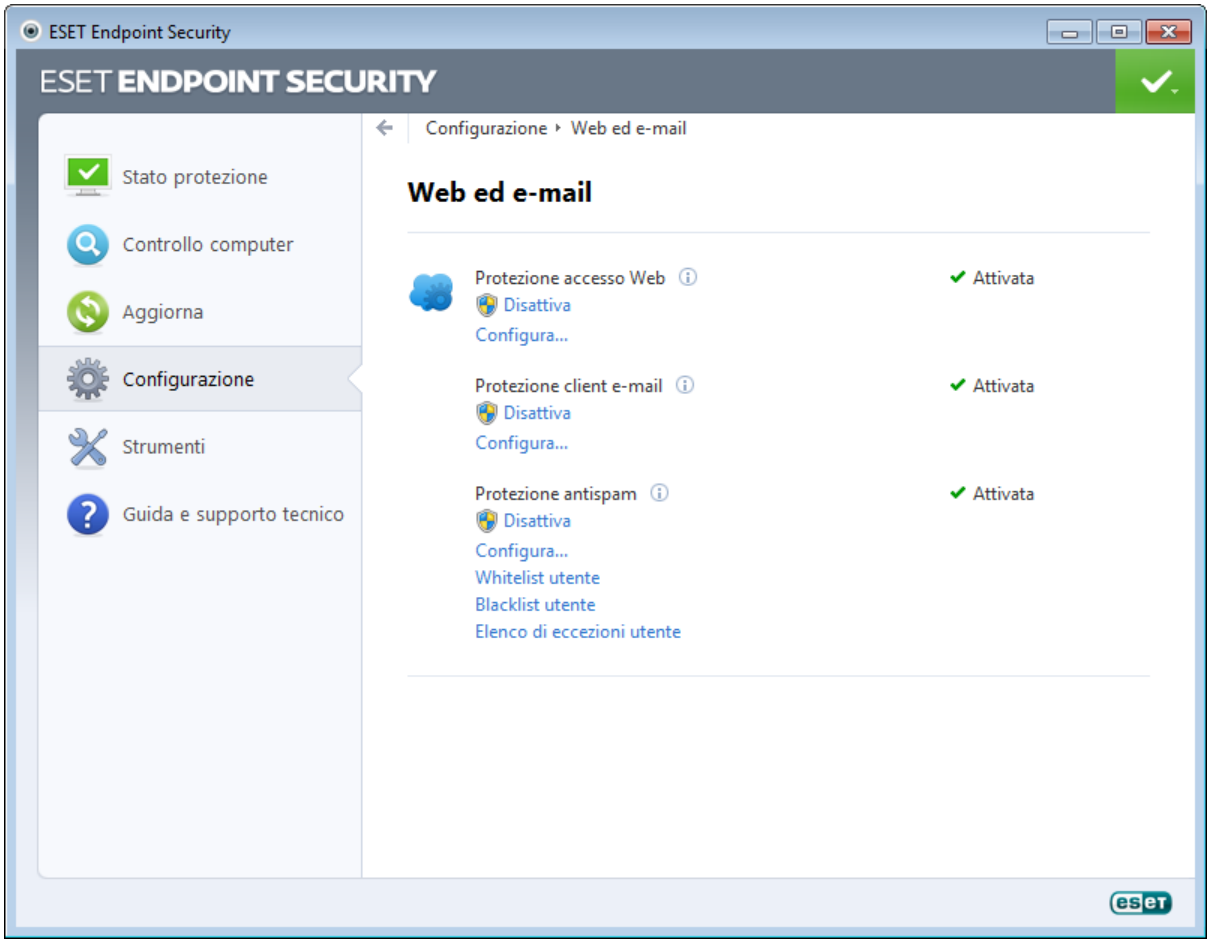
Il Firewall personale ESET Endpoint Security funziona su diversi livelli:

- **Tutte le funzioni attive** - Il Firewall è completamente integrato e i rispettivi componenti sono attivi (opzione predefinita). Si consiglia di lasciare attivata questa opzione se il computer è collegato a una rete molto ampia o a Internet. Si tratta dell'opzione più sicura e protegge completamente il sistema.
- **Firewall non attivo** - Il Firewall è integrato nel sistema e media la comunicazione di rete ma non esegue il controllo delle minacce.
- **Esegui scansione solo dei protocolli di applicazioni** - Sono attivi solo i componenti del Firewall che eseguono il controllo dei protocolli delle applicazioni (HTTP, POP3, IMAP e le rispettive versioni protette). Se i protocolli delle applicazioni non vengono controllati, la protezione viene applicata a livello di Protezione file system in tempo reale e Controllo del computer su richiesta.
- **Firewall personale completamente disattivato** - Selezionare questa opzione per annullare completamente la registrazione del Firewall personale dal sistema. Non verrà eseguito alcun controllo. Può essere utile durante la verifica: se un'applicazione è bloccata, è possibile controllare se è bloccata dal firewall. Si tratta dell'opzione meno sicura ed è quindi consigliabile prestare la massima attenzione quando si disattiva completamente il firewall.

Rimanda l'aggiornamento del modulo firewall fino al prossimo avvio del computer - L'aggiornamento viene solo scaricato. L'installazione verrà infatti eseguita al riavvio del computer.

4.3 Web ed e-mail

Le opzioni di configurazione del Web ed e-mail sono disponibili nel riquadro **Configurazione** facendo clic sul titolo **Web ed e-mail**. Da qui è possibile accedere alle impostazioni dettagliate del programma.



La connettività Internet è una funzione standard dei personal computer. Purtroppo è diventato anche lo strumento principale per il trasferimento di codice dannoso. Per tale motivo, è essenziale gestire in modo accurato la **Protezione accesso Web**.

La **Protezione client e-mail** garantisce il controllo delle comunicazioni via e-mail ricevute mediante il protocollo POP3 e IMAP. Utilizzando il programma plug-in per il client e-mail in uso, ESET Endpoint Security controlla tutte le comunicazioni dal client e-mail (POP3, MAPI, IMAP, HTTP).

La **Protezione antispam** consente di filtrare i messaggi e-mail indesiderati.

Disattiva - Consente di disattivare la protezione Web/e-mail/antispam per i client e-mail.

Configurazione ... - Consente di accedere alla configurazione avanzata della protezione Web/e-mail/antispam .

Whitelist utente - Apre una finestra di dialogo che consente di aggiungere, modificare o eliminare indirizzi e-mail considerati sicuri. I messaggi e-mail provenienti da un indirizzo presente nella whitelist non verranno sottoposti alla scansione alla ricerca di spamming.

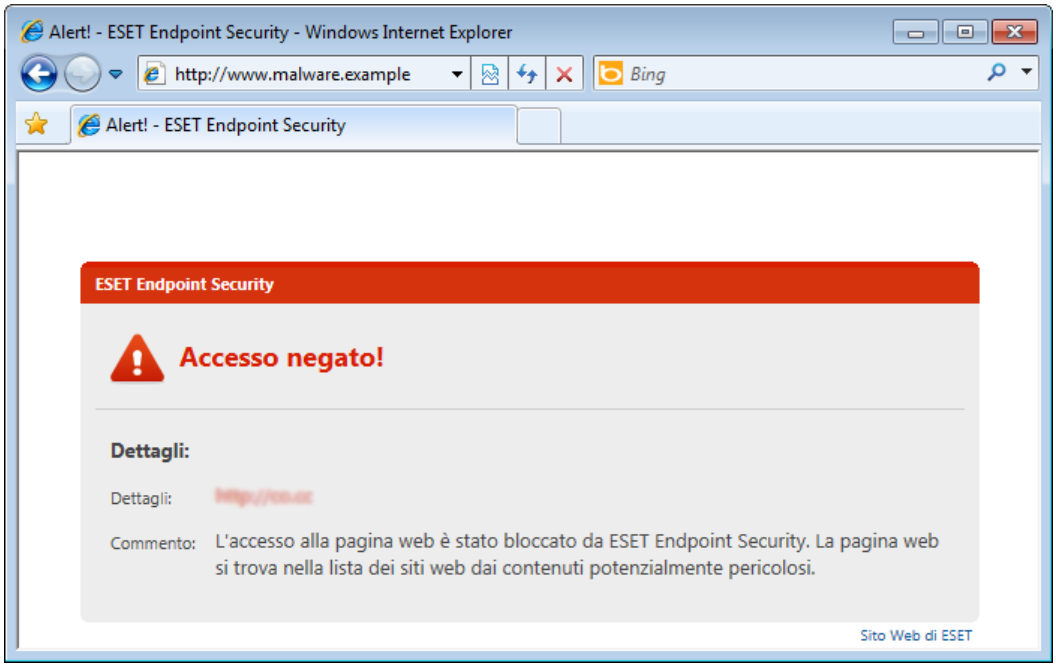
Blacklist utente - Apre una finestra di dialogo che consente di aggiungere, modificare o eliminare indirizzi e-mail considerati non sicuri. I messaggi e-mail provenienti da un indirizzo presente nella blacklist verranno considerati come spamming.

Elenco di eccezioni utente - Apre una finestra di dialogo che consente di aggiungere, modificare o eliminare indirizzi e-mail che potrebbero essere contraffatti e usati per inviare messaggi di spamming. I messaggi e-mail provenienti da un indirizzo presente nell'elenco di eccezioni utenti verranno sempre sottoposti alla scansione alla ricerca di spamming. Per impostazione predefinita, l'elenco di eccezioni contiene gli indirizzi e-mail degli account del client e-mail esistenti.

4.3.1 Protezione accesso Web

La connettività Internet è una funzione standard in un personal computer. Purtroppo è diventato anche lo strumento principale per il trasferimento di codice dannoso. Protezione accesso Web monitora la comunicazione tra i browser Internet e i server remoti ed è conforme alle regole HTTP (Hypertext Transfer Protocol) e HTTPS (comunicazione crittografata).

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni confidenziali). Per ulteriori informazioni su questa attività, consultare il glossario. ESET Endpoint Security supporta la protezione antiphishing, ovvero le pagine Web note con tale contenuto sono sempre bloccate.


Alert! - ESET Endpoint Security - Windows Internet Explorer
http://www.malware.example
Bing
Alert! - ESET Endpoint Security
ESET Endpoint Security
Accesso negato!
Dettagli:
Dettagli:
Commento:
L'accesso alla pagina web è stato bloccato da ESET Endpoint Security. La pagina web si trova nella lista dei siti web dai contenuti potenzialmente pericolosi.
Sito Web di ESET

Si consiglia di attivare la Protezione accesso Web . L'opzione è disponibile dalla finestra principale di ESET Endpoint Security accedendo a **Configurazione** > **Web ed e-mail** > **Protezione accesso Web**.

4.3.1.1 HTTP, HTTPS

Per impostazione predefinita, ESET Endpoint Security è configurato in modo da utilizzare gli standard della maggior parte dei browser Internet. Le opzioni di impostazione dello scanner HTTP possono tuttavia essere modificate in **Configurazione avanzata** (F5) > **Web ed e-mail** > **Protezione accesso Web** > **HTTP, HTTPS**. Nella finestra principale **Scanner HTTP/HTTPS** è possibile selezionare o deselezionare l'opzione **Attiva controllo HTTP**. È inoltre possibile definire i numeri delle porte utilizzate per la comunicazione HTTP. L'impostazione predefinita per i numeri delle porte è 80 (HTTP), 8080 e 3128 (per il server proxy).

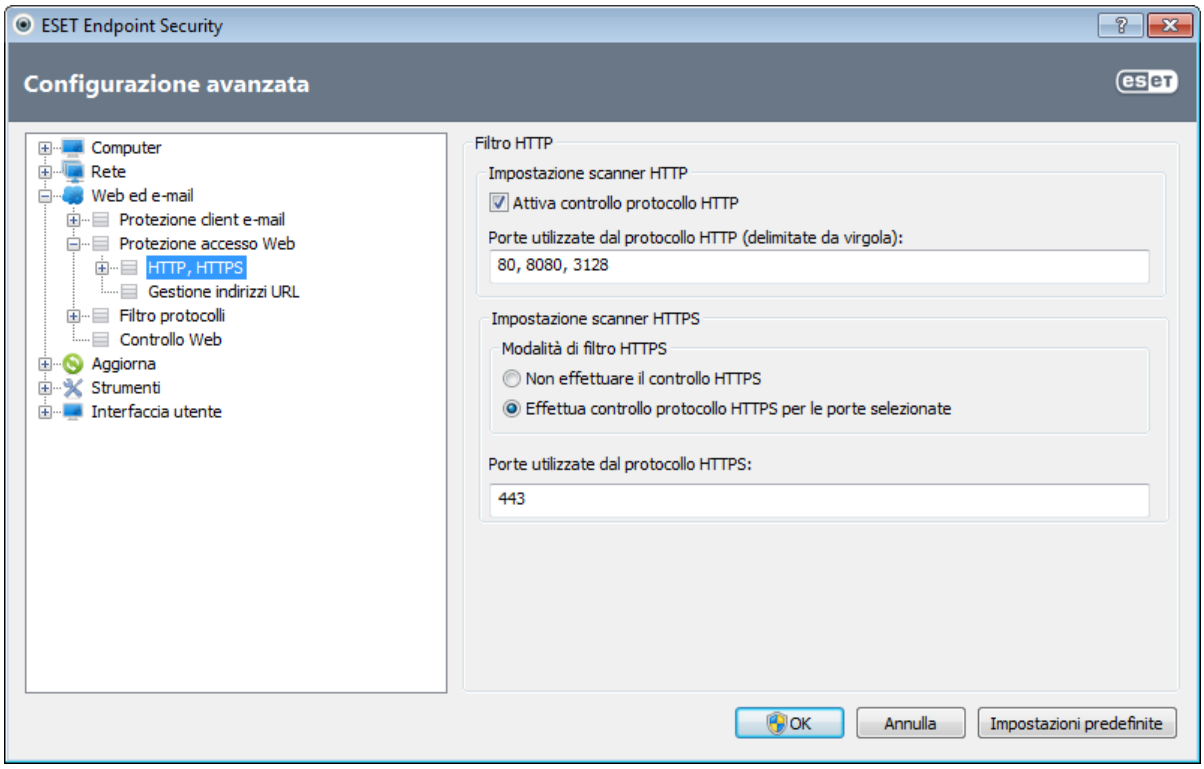
ESET Endpoint Security supporta il controllo del protocollo HTTPS. La comunicazione HTTPS utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET Endpoint Security controlla le comunicazioni utilizzando i metodi di crittografia SSL (Secure Socket Layer) e TLS (Transport Layer Security). Il controllo HTTPS può essere impostato con le seguenti modalità:

Non effettuare il controllo del protocollo HTTPS - La comunicazione crittografata non verrà controllata.

Effettua il controllo del protocollo HTTPS per le porte selezionate - Il controllo HTTPS viene utilizzato solo per le porte definite in **Porte utilizzate dal protocollo HTTPS**.

Effettua il controllo del protocollo HTTPS per le porte selezionate - Il programma eseguirà il controllo solo sulle applicazioni specificate nella sezione browser e che utilizzano le porte definite in **Porte utilizzate dal protocollo HTTPS**. La porta 443 rappresenta l'impostazione predefinita.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a Verifica protocollo SSL nella sezione Configurazione avanzata, fare clic su **Web ed e-mail** > **Filtro protocolli** > **SSL** e selezionare l'opzione **Effettua sempre la scansione del protocollo SSL**.



4.3.1.1.1 Modalità attiva per i browser Internet

ESET Endpoint Security contiene anche il sottomenu **Modalità attiva** che definisce la modalità di controllo per i browser Web.

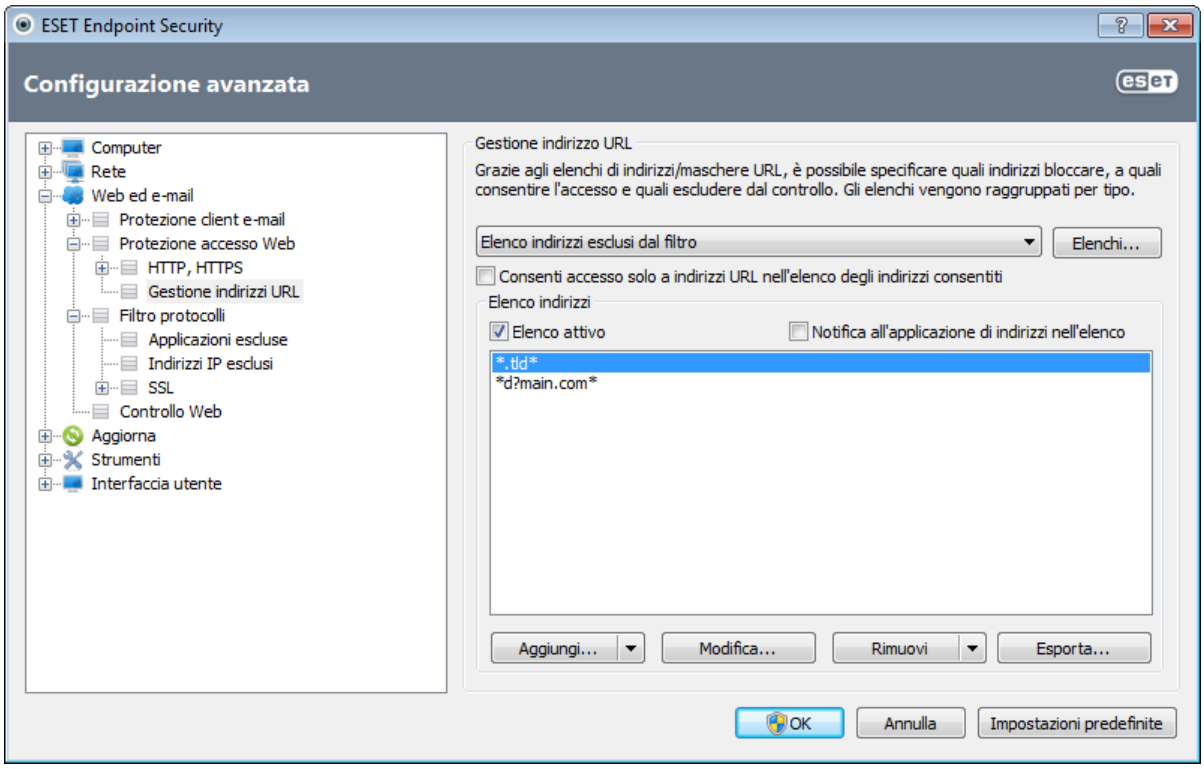
La **Modalità attiva** è utile in quanto consente la verifica dell'insieme dei dati trasferiti dalle applicazioni che accedono a Internet, indipendentemente dal fatto che siano contrassegnati o meno come browser Internet (per ulteriori informazioni, consultare Web e client e-mail). Se la Modalità attiva è disattivata, la comunicazione delle applicazioni viene monitorata gradualmente in batch. Questo può ridurre l'efficacia del processo di verifica dei dati, ma fornisce anche una maggiore compatibilità per le applicazioni elencate. Se non si verificano problemi durante il relativo utilizzo, è consigliabile attivare la modalità attiva di controllo selezionando al casella di controllo accanto all'applicazione desiderata. Di seguito è descritto il funzionamento della Modalità attiva: quando un'applicazione controllata scarica dei dati, questi vengono salvati in un file temporaneo creato da ESET Endpoint Security. In quel momento, i dati non sono disponibili per l'applicazione specifica. Una volta che il download è stato completato, i dati vengono controllati per rilevare il codice dannoso. Se non vengono trovate infiltrazioni, i dati vengono inviati all'applicazione originale. Questo processo fornisce un controllo completo delle comunicazioni effettuate da un'applicazione controllata. Se è attivata la modalità passiva, i dati vengono inviati man mano all'applicazione originale per evitare timeout.

4.3.1.2 Gestione indirizzo URL

La sezione Gestione indirizzo URL consente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo. I pulsanti **Aggiungi**, **Modifica**, **Rimuovi** ed **Esporta** vengono utilizzati per gestire l'elenco degli indirizzi. Non sarà possibile accedere ai siti Web presenti nell'elenco degli indirizzi bloccati. Durante l'accesso, i siti Web presenti nell'elenco degli indirizzi esclusi non vengono sottoposti al controllo per rilevare il codice dannoso. Se è attivata l'opzione **Consenti accesso solo a indirizzi URL nell'elenco degli indirizzi consentiti**, sarà possibile accedere solo agli indirizzi presenti nell'elenco degli indirizzi consentiti, mentre gli altri indirizzi HTTP verranno bloccati.

Se si aggiunge un indirizzo URL all'**Elenco indirizzi esclusi dal filtro**, l'indirizzo verrà escluso dal controllo. È inoltre possibile consentire o bloccare determinati indirizzi aggiungendoli all'**Elenco di indirizzi consentiti** o all'**Elenco di indirizzi bloccati**. Dopo aver selezionato il pulsante **Elenchi...**, verrà visualizzata la finestra **Elenchi indirizzi/maschere HTTP** in cui è possibile selezionare le opzioni **Aggiungi** o **Rimuovi** per aggiungere o rimuovere elenchi di indirizzi. Per aggiungere un indirizzo URL HTTPS all'elenco, è necessario che l'opzione **Effettua sempre scansione del protocollo SSL** sia attiva.

In tutti gli elenchi è possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri, mentre il punto interrogativo sostituisce qualsiasi simbolo. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, poiché l'elenco deve contenere solo indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente. Per attivare l'elenco, selezionare l'opzione **Elenco attivo**. Se si desidera ricevere una notifica quando viene immesso un indirizzo dall'elenco corrente, selezionare **Notifica all'applicazione di indirizzi nell'elenco**.



Aggiungi.../Da file - Consente di aggiungere un indirizzo all'elenco, manualmente (**Aggiungi**) o da un semplice file di testo (**Da file**). L'opzione **Da file** consente di aggiungere più indirizzi URL/maschere che vengono salvati in un file di testo.

Modifica... - Consente di modificare manualmente gli indirizzi, ad esempio aggiungendo una maschera ("*" e "?").

Rimuovi/Rimuovi tutto - Fare clic su **Rimuovi** per rimuovere l'indirizzo selezionato dall'elenco. Per rimuovere tutti gli indirizzi, selezionare **Rimuovi tutto**.

Esporta... - Consente di salvare gli indirizzi dall'elenco corrente in un file di testo.

4.3.2 Protezione client di posta

La Protezione client e-mail garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP. Utilizzando il plug-in per Microsoft Outlook e altri client e-mail, ESET Endpoint Security controlla tutte le comunicazioni dal client e-mail (POP3, MAPI, IMAP, HTTP). Durante la verifica dei messaggi in arrivo, vengono utilizzati tutti i metodi di scansione avanzata forniti dal motore di scansione ThreatSense. Ciò significa che il rilevamento di programmi dannosi viene eseguito ancora prima del confronto con il database delle firme antivirali. La scansione delle comunicazioni mediante i protocolli POP3 e IMAP non dipende dal client e-mail in uso.

Le opzioni per questa funzionalità sono disponibili nella sezione **Configurazione avanzata** > **Web ed e-mail** > **Protezione client e-mail**.

Configurazione parametri motore ThreatSense - La configurazione avanzata dello scanner antivirus consente di configurare gli oggetti da controllare, i metodi di rilevamento e così via. Fare clic su **Configurazione...** per visualizzare la finestra della configurazione dettagliata dello scanner antivirus.

Dopo che un messaggio e-mail è stato controllato, una notifica contenente i risultati di scansione può essere aggiunta al messaggio. È possibile selezionare **Aggiungi notifiche alle e-mail ricevute e lette**, nonché **Aggiungi notifica alle e-mail inviate**. Tali notifiche non possono essere ritenute completamente affidabili poiché potrebbero essere omesse in messaggi HTML problematici o essere create da determinati virus. Le notifiche possono essere aggiunte alle e-mail ricevute e lette, a quelle inviate o entrambe. Le opzioni disponibili sono:

- **Mai** - Non viene aggiunta alcuna notifica.
- **Solo per l'e-mail infetta** - Solo i messaggi contenenti software dannoso vengono contrassegnati come controllati (impostazione predefinita).
- **Per tutte le e-mail** - Il programma aggiunge la notifica a tutte le e-mail sottoposte a scansione.

Aggiungi nota all'oggetto di e-mail infette ricevute e lette/inviate - Selezionare questa casella di controllo se si desidera che la protezione e-mail includa un allarme antivirus nell'oggetto di un'e-mail infetta. Questa funzione consente di filtrare in modo semplice le e-mail infette in base all'oggetto (se supportata dal programma e-mail in uso). Aumenta inoltre il livello di credibilità del destinatario e se viene rilevata un'infiltrazione, fornisce informazioni utili sul

livello di minaccia di un determinato messaggio e-mail o mittente.

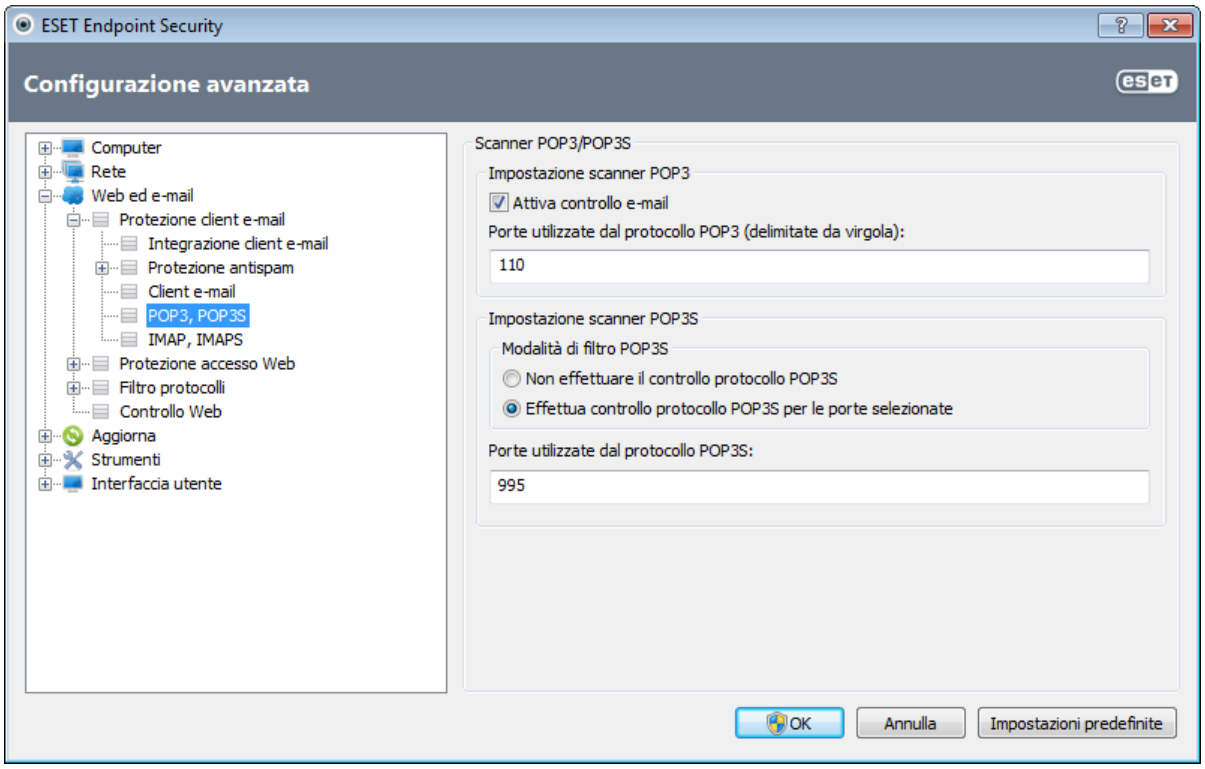
Template aggiunto all'oggetto dell'e-mail infetta - Modificare questo template se si desidera cambiare il formato predefinito dell'oggetto di un'e-mail infetta. Questa funzione sostituirà l'oggetto del messaggio "Ciao" con un determinato valore predefinito "[virus]" nel seguente formato: "[virus] Ciao". La variabile %VIRUSNAME% rappresenta la minaccia rilevata.

4.3.2.1 Filtro POP3, POP3S

Il protocollo POP3 è quello più diffuso per la ricezione di comunicazioni e-mail in un'applicazione client e-mail. ESET Endpoint Security offre la protezione per questo protocollo, indipendentemente dal client e-mail in uso.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Perché il modulo funzioni correttamente, verificare che sia attivato: il controllo del protocollo POP3 viene eseguito automaticamente senza che sia necessario riconfigurare il client e-mail. Per impostazione predefinita, vengono sottoposte a scansione tutte le comunicazioni della porta 110, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a Verifica protocollo SSL nella sezione Configurazione avanzata, fare clic su **Web ed e-mail** > **Filtro protocolli** > **SSL** e selezionare l'opzione **Effettua sempre la scansione del protocollo SSL**.



In questa sezione è possibile configurare il controllo dei protocolli POP3 e POP3S.

Attiva controllo e-mail - Se questa opzione è attivata, tutto il traffico POP3 viene monitorato per rilevare il software dannoso

Porte utilizzate dal protocollo POP3 - Elenco delle porte usate dal protocollo POP3 (110 per impostazione predefinita).

ESET Endpoint Security supporta anche il controllo del protocollo POP3S. Questo tipo di comunicazione utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET Endpoint Security controlla le comunicazioni utilizzando i metodi di crittografia SSL (Secure Socket Layer) e TLS (Transport Layer Security).

Non effettuare il controllo POP3S - La comunicazione crittografata non verrà controllata.

Effettua controllo protocollo POP3S per le porte selezionate - Selezionare questa opzione per attivare il controllo POP3S solo per le porte definite in **Porte utilizzate dal protocollo POP3S**.

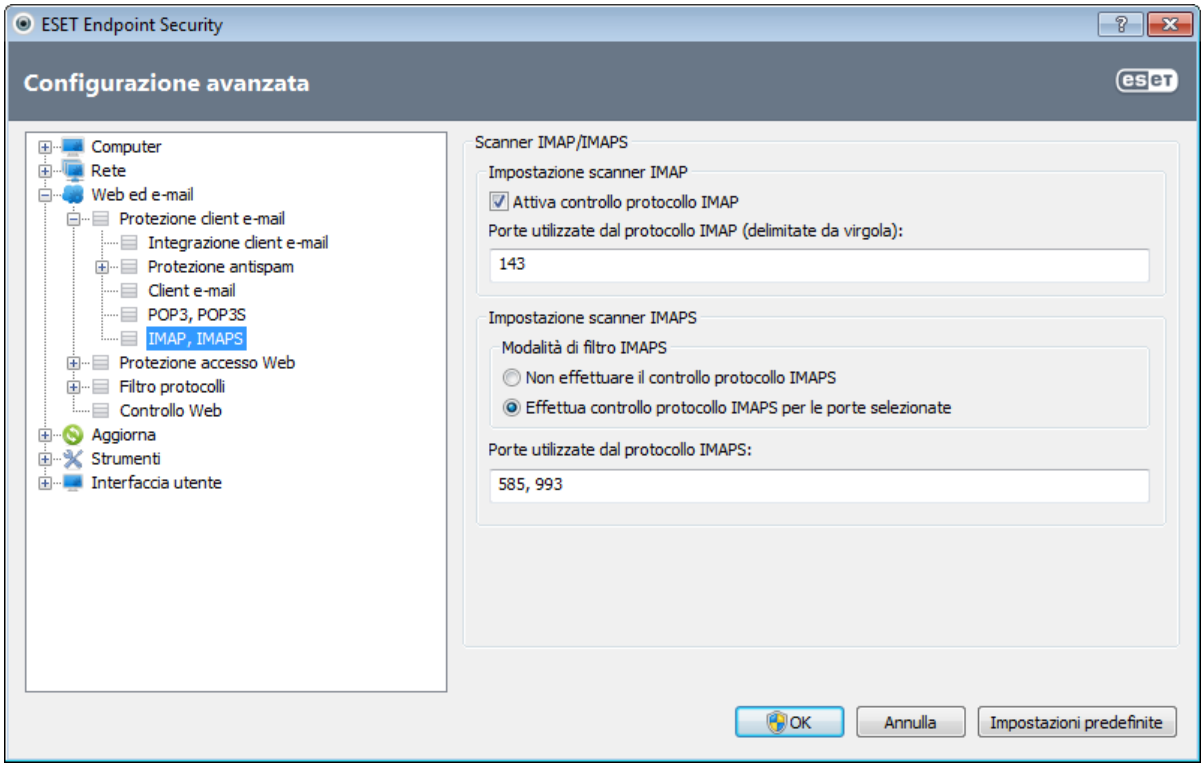
Porte utilizzate dal protocollo POP3S - Elenco delle porte POP3S da controllare (995 per impostazione predefinita).

4.3.2.2 Controllo protocolli IMAP, IMAPS

IMAP (Internet Message Access Protocol) è un altro protocollo Internet per il recupero dei messaggi e-mail. Il protocollo IMAP offre alcuni vantaggi rispetto al protocollo POP3: ad esempio più client possono connettersi simultaneamente alla stessa casella di posta e mantenere informazioni sullo stato del messaggio (se il messaggio è stato letto, eliminato o è stata inviata una risposta). ESET Endpoint Security offre la protezione per questo protocollo, indipendentemente dal client e-mail in uso.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Perché il modulo funzioni correttamente, verificare che sia attivato: il controllo del protocollo IMAP viene eseguito automaticamente senza che sia necessario riconfigurare il client e-mail. Per impostazione predefinita, vengono sottoposte a scansione tutte le comunicazioni della porta 143, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a Verifica protocollo SSL nella sezione Configurazione avanzata, fare clic su **Web ed e-mail** > **Filtro protocolli** > **SSL** e selezionare l'opzione **Effettua sempre la scansione del protocollo SSL**.

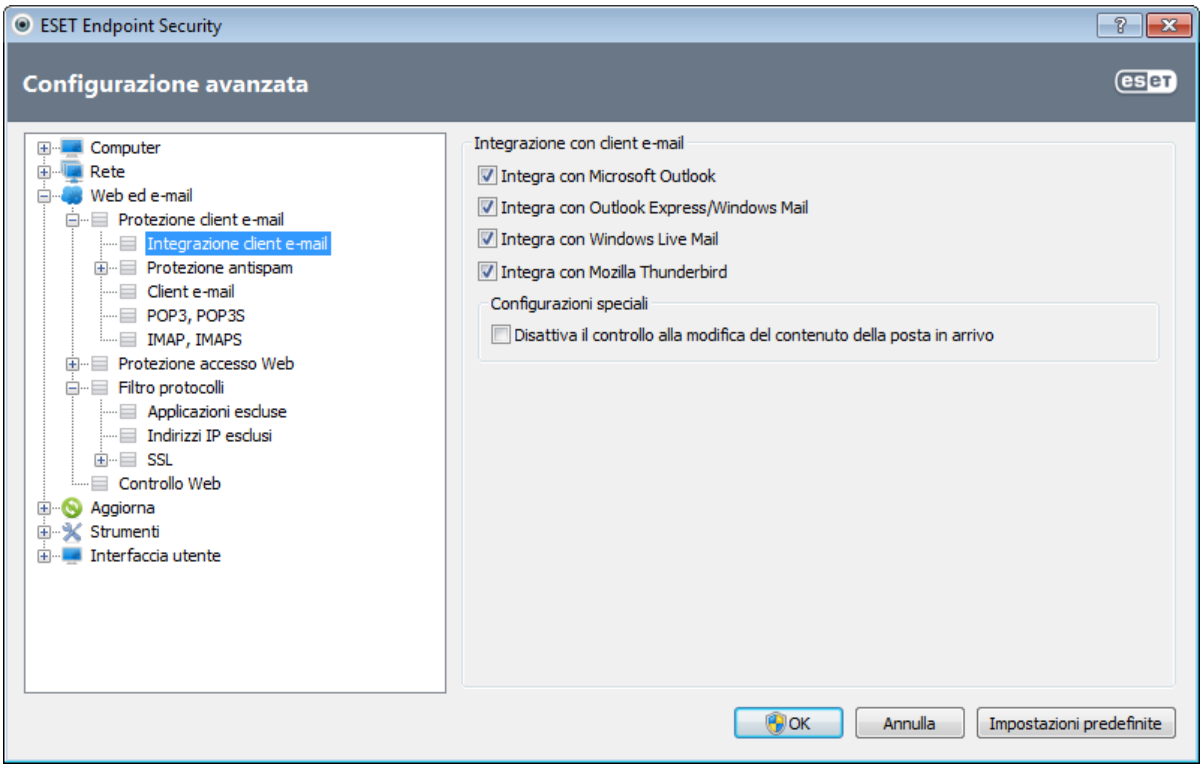


4.3.2.3 Integrazione con client di posta

L'integrazione di ESET Endpoint Security con i client e-mail aumenta il livello di protezione attiva contro codici dannosi nei messaggi e-mail. Se il client e-mail in uso è supportato, tale integrazione può essere attivata in ESET Endpoint Security. Se l'integrazione viene attivata, la barra degli strumenti di ESET Endpoint Security viene inserita direttamente nel client e-mail, consentendo una protezione e-mail più efficace. Le impostazioni di integrazione sono disponibili nella sezione **Configurazione** > **Accedi a configurazione avanzata...** > **Web ed e-mail** > **Protezione client e-mail** > **Integrazione con client e-mail**.

I client e-mail attualmente supportati includono Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird. Per un elenco completo dei client e-mail supportati e delle relative versioni, fare riferimento al seguente articolo della Knowledge Base ESET.

Selezionare la casella di controllo accanto a **Disattiva il controllo alla modifica del contenuto della posta in arrivo** se si riscontra un rallentamento del sistema durante l'utilizzo del client e-mail. Una situazione simile può verificarsi durante il download dei messaggi e-mail da Kerio Outlook Connector Store.



Anche se l'integrazione non è attivata, la comunicazione e-mail rimane comunque protetta tramite il modulo di protezione client e-mail (POP3, IMAP).

4.3.2.3.1 Configurazione della protezione client di posta

Il modulo di protezione client e-mail supporta i seguenti client e-mail: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird. Per questi programmi la protezione e-mail esegue la stessa funzione di un plugin. Il vantaggio principale offerto dal controllo plugin consiste nel fatto che non sia dipendente dal protocollo utilizzato. Quando il client e-mail riceve un messaggio crittografato, questo viene decodificato e inviato al programma di scanner antivirus.

E-mail per il controllo

E-mail ricevute - Attiva/disattiva la verifica dei messaggi ricevuti.
E-mail inviate - Attiva/disattiva la verifica dei messaggi inviati.
E-mail lette - Attiva/disattiva la verifica dei messaggi letti.

Azione da eseguire sull'e-mail infetta

Nessuna azione - Se questa opzione è attivata, il programma identificherà gli allegati infetti senza tuttavia eseguire alcuna azione.
Elimina e-mail - Il programma notificherà all'utente le eventuali infiltrazioni ed eliminerà il messaggio.
Sposta e-mail nella cartella Posta eliminata - I messaggi e-mail infetti verranno spostati automaticamente nella cartella **Posta eliminata**.
Sposta e-mail nella cartella - Specificare la cartella personalizzata in cui si desidera spostare il messaggio e-mail infetto quando viene rilevato.

Altro

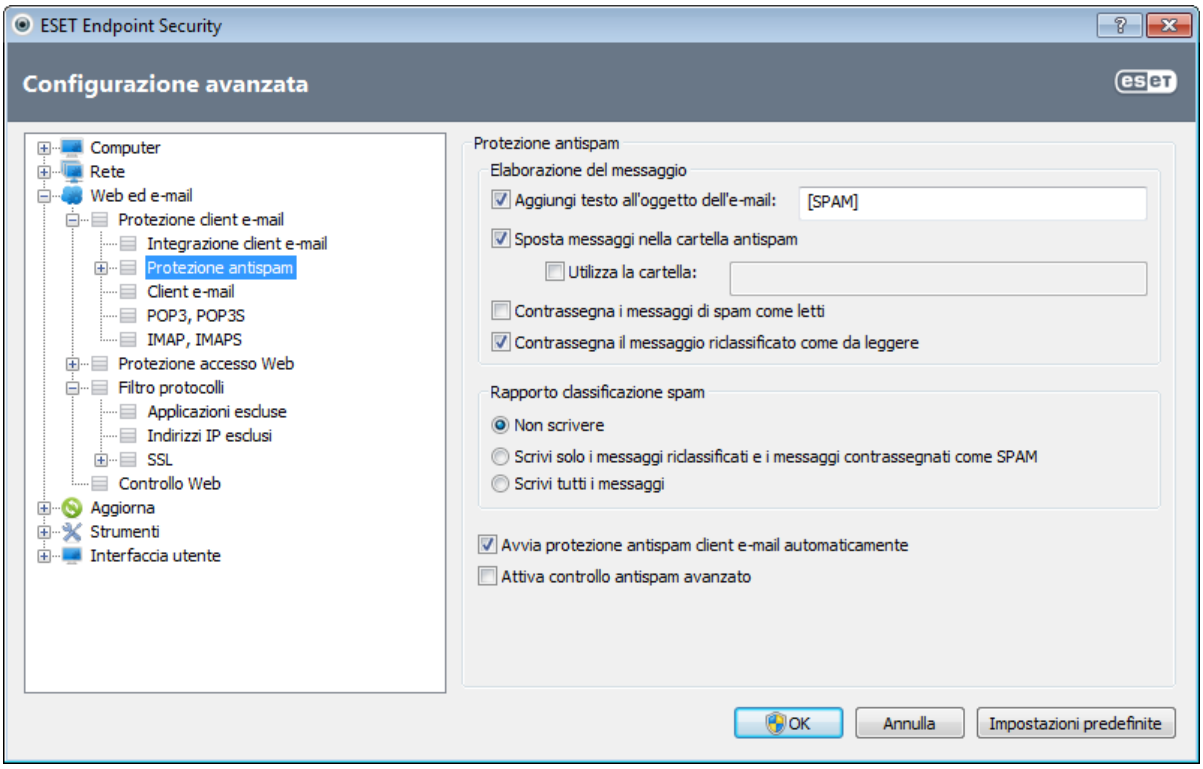
Ripeti controllo dopo l'aggiornamento - Attiva/disattiva un nuovo controllo dopo l'aggiornamento del database delle firme antivirali.
Accetta i risultati del controllo da altri moduli - Se questa opzione è selezionata, il modulo di protezione e-mail accetta i risultati del controllo di altri moduli di protezione.

4.3.2.4 Eliminazione delle infiltrazioni

In caso di ricezione di messaggi e-mail infetti, verrà visualizzata una finestra di avviso contenente il nome del mittente, il messaggio e-mail e il nome dell'infiltrazione. Nella parte inferiore della finestra, sono disponibili le opzioni **Pulisci**, **Elimina** o **Nessuna azione** per l'oggetto rilevato. Nella maggior parte dei casi è consigliabile selezionare **Pulisci** o **Elimina**. In alcuni casi, si desidera comunque ricevere il file infetto, selezionare **Nessuna azione**. Se è attivata l'opzione **Massima pulizia**, verrà visualizzata una finestra di informazioni, senza nessuna opzione disponibile per gli oggetti infetti

4.3.3 Protezione antispam

I messaggi e-mail non desiderati, definiti spam, costituiscono uno dei maggiori problemi delle comunicazioni elettroniche. Rappresentano infatti quasi l'80% di tutte le comunicazioni e-mail. La protezione antispam consente di prevenire questo problema. Associando una serie di principi molto efficaci, il modulo antispam offre un filtraggio di livello superiore per mantenere pulita la cartella Posta in arrivo.



Un principio essenziale per il rilevamento dello spam è la capacità di riconoscere messaggi indesiderati in base a indirizzi affidabili predefiniti (whitelist) e a indirizzi di spam (blacklist). Tutti gli indirizzi dell'elenco contatti dell'utente vengono aggiunti automaticamente alla whitelist, oltre a tutti gli altri indirizzi contrassegnati dall'utente come sicuri.

Il metodo principale per rilevare lo spam consiste nella scansione delle proprietà di un messaggio e-mail. I messaggi ricevuti vengono sottoposti a scansione secondo i criteri antispam di base (definizioni di messaggi, euristica statistica, riconoscimento di algoritmi e altri metodi univoci) e dal valore di indice risultante è possibile determinare se un messaggio è spam o meno.

La protezione Antispam in ESET Endpoint Security consente di impostare differenti parametri per gestire le mailing list. Le opzioni disponibili sono le seguenti:

Avvia protezione antispam client e-mail automaticamente - Consente di attivare/disattivare la protezione antispam del client e-mail.

Elaborazione del messaggio

Aggiungi testo all'oggetto dell'e-mail - Consente di aggiungere una stringa di testo predefinita e personalizzata nell'oggetto dei messaggi classificati come spam. La stringa predefinita è "[SPAMMING]".

Sposta messaggi nella cartella antispam - Se questa opzione è selezionata, i messaggi di spam verranno spostai nella cartella predefinita per la posta indesiderata.

Utilizza la cartella - Questa opzione sposta i messaggi di spam in una cartella definita dall'utente.

Contrassegna i messaggi di spam come letti - Scegliere questa opzione per contrassegnare automaticamente come

letti i messaggi di spam. Consente di mettere in evidenza solo i messaggi "puliti".

Contrassegna il messaggio riclassificato come da leggere - I messaggi originariamente classificati come spam ma contrassegnati come "puliti" in un secondo tempo verranno visualizzati come da leggere.

Rapporto classificazione spam

Il motore Antispam di ESET Endpoint Security assegna un classificazione di spam a ogni messaggio sottoposto a scansione. Il messaggio verrà registrato nel rapporto antispam (**ESET Endpoint Security** > **Strumenti** > **File di rapporto** > **Protezione antispam**).

- **Non scrivere** - La cella **Classificazione** nel rapporto di protezione Antispam sarà vuota.
- **Scrivi solo i messaggi riclassificati e i messaggi contrassegnati come SPAM** - Usare questa opzione per registrare una classificazione di spam per i messaggi contrassegnati come SPAM.
- **Scrivi tutti i messaggi** - Tutti i messaggi verranno registrati sul rapporto con una classificazione di spam.

Avvia protezione antispam client e-mail automaticamente - Se questa opzione è selezionata, la protezione antispam verrà attivata automaticamente all'avvio del sistema.

Attiva controllo antispam avanzato - Verranno scaricati database antispam aggiuntivi, con conseguente miglioramento delle capacità antispam e dei risultati.

ESET Endpoint Security supporta la protezione Antispam per Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

4.3.3.1 Aggiunta di indirizzi alla whitelist e alla blacklist

Gli indirizzi e-mail appartenenti alle persone con le quali si comunica frequentemente possono essere aggiunti alla whitelist per essere certi che nessun messaggio proveniente da un indirizzo presente nella whitelist sia classificato come spam. Gli indirizzi spam noti possono essere aggiunti alla blacklist ed essere sempre classificati come spam. Per aggiungere un nuovo indirizzo alla whitelist o alla blacklist, fare clic con il pulsante destro del mouse sul messaggio e-mail e selezionare **ESET Endpoint Security** > **Aggiungi alla whitelist** o **Aggiungi alla blacklist**, oppure fare clic sul pulsante **Indirizzo affidabile** o **Indirizzo spam** sulla barra degli strumenti antispam di ESET Endpoint Security nel client e-mail.

Questa procedura è applicabile anche agli indirizzi spam. Se un indirizzo e-mail viene riportato nella blacklist, tutti i messaggi e-mail provenienti da questo indirizzo saranno classificati come spam.

4.3.3.2 Contrassegnare messaggi come spam

Qualsiasi messaggio visualizzato nel client e-mail può essere contrassegnato come spam. A tale scopo, fare clic con il pulsante destro del mouse sul messaggio e selezionare **ESET Endpoint Security** > **Riclassifica messaggi selezionati come spam** oppure fare clic su **Indirizzo spam** sulla barra degli strumenti antispam di ESET Endpoint Security nella parte superiore del client e-mail.

I messaggi riclassificati vengono spostati automaticamente nella cartella SPAM, ma l'indirizzo e-mail del mittente non viene aggiunto alla blacklist. Allo stesso modo, i messaggi possono essere classificati come "non spam". Se i messaggi della cartella **Posta indesiderata** vengono classificati come non spam, verranno spostati nella relativa cartella originale. Se un messaggio viene contrassegnato come non spam, l'indirizzo del mittente non viene automaticamente aggiunto alla whitelist.

4.3.4 Filtraggio protocolli

La protezione antivirus per i protocolli dell'applicazione viene fornita tramite il motore di scansione di ThreatSense, che integra perfettamente tutte le tecniche di scansione avanzata dei malware. Il controllo funziona automaticamente, indipendentemente dal browser o dal client e-mail in uso. Per la comunicazione crittografata (SSL) vedere **Filtro protocolli** > **SSL**.

Attiva filtro del contenuto del protocollo di applicazioni - Se questa opzione è attivata, tutto il traffico HTTP(S), POP3(S) e IMAP(S) verrà controllato dallo scanner antivirus.

NOTA: in Windows Vista Service Pack 1 e Windows 7 per il controllo delle comunicazioni di rete viene utilizzata la nuova architettura Windows Filtering Platform (WFP). Poiché la tecnologia WPF fa uso di tecniche di monitoraggio particolari, le opzioni seguenti non sono disponibili:

- **Porte HTTP e POP3** – Consente di limitare l'instradamento del traffico sul server proxy interno solo alle porte HTTP e POP3.
- **Applicazioni contrassegnate come browser Internet e client e-mail** - Consente di limitare l'instradamento del traffico sul server proxy interno solo alle applicazioni contrassegnate come browser e client e-mail (**Web ed e-mail** > **Filtro protocolli** > **Web e client e-mail**).
- **Porte e applicazioni contrassegnate come browser Internet o client e-mail** – Consente l'instradamento di tutto il traffico sulle porte HTTP e POP3 oltre che delle comunicazioni delle applicazioni contrassegnate come browser e client e-mail sul server proxy interno.

4.3.4.1 Web e client di posta

NOTA: in Windows Vista Service Pack 1 e Windows 7 per il controllo delle comunicazioni di rete viene utilizzata la nuova architettura Windows Filtering Platform (WFP). Poiché la tecnologia WPF fa uso di tecniche di monitoraggio particolari, la sezione **Web e client e-mail** non è disponibile.

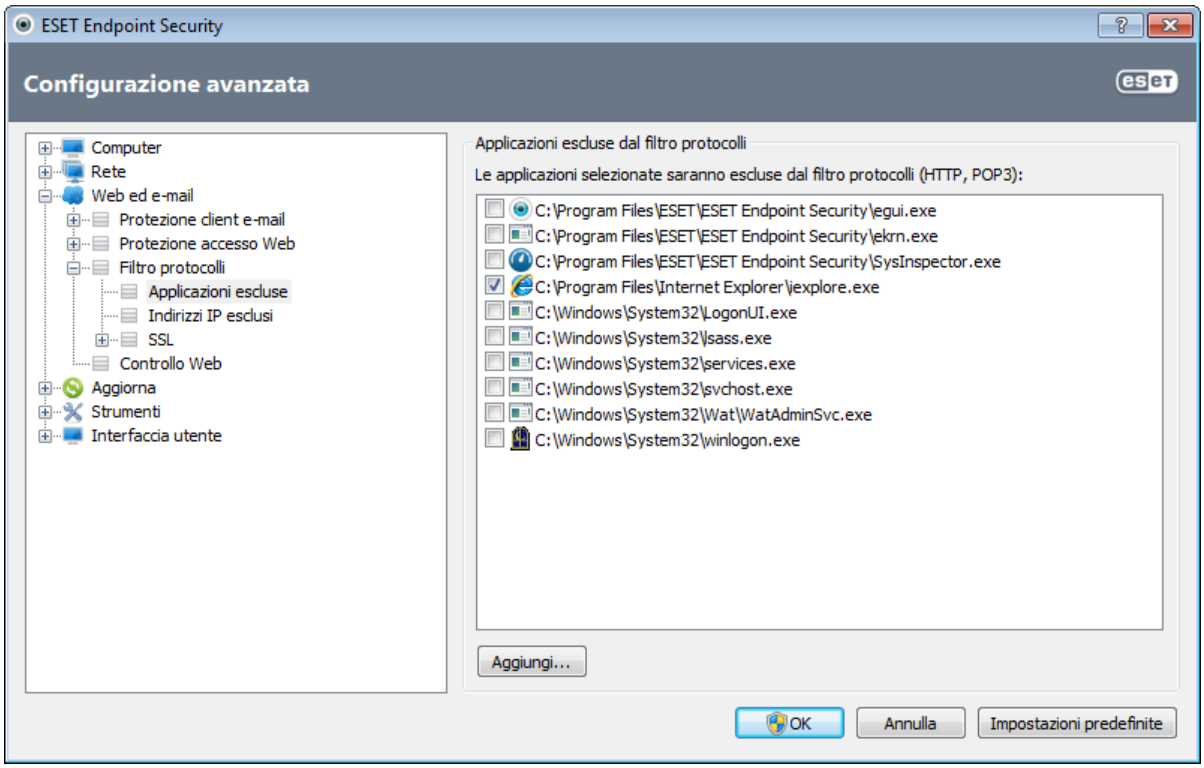
A causa dell'enorme quantità di codice dannoso che circola su Internet, una navigazione Internet sicura è essenziale per la protezione del computer. Le vulnerabilità dei browser Web e i collegamenti fraudolenti aiutano il codice dannoso a penetrare inosservato nel sistema. Per tale motivo, ESET Endpoint Security si focalizza sulla sicurezza dei browser Web. Ogni applicazione che accede alla rete può essere contrassegnata come un browser. La casella di controllo presenta due stati:

- **Senza segno di spunta** - La comunicazione delle applicazioni viene filtrata solo per le porte specificate.
- **Con segno di spunta** - La comunicazione viene sempre filtrata (anche se viene impostata una porta differente).

4.3.4.2 Applicazioni escluse

Per escludere la comunicazione di specifiche applicazioni di rete dal filtraggio dei contenuti, selezionarle nell'elenco. Sulla comunicazione HTTP/POP3/IMAP delle applicazioni selezionate non verrà eseguito il rilevamento delle minacce. È consigliabile usare questa opzione solo per le applicazioni che non funzionano correttamente se la rispettiva comunicazione viene sottoposta a controllo.

L'esecuzione di applicazioni e servizi sarà disponibile automaticamente. Fare clic sul pulsante **Aggiungi...** per selezionare manualmente un'applicazione non visualizzata sull'elenco del filtro protocolli.

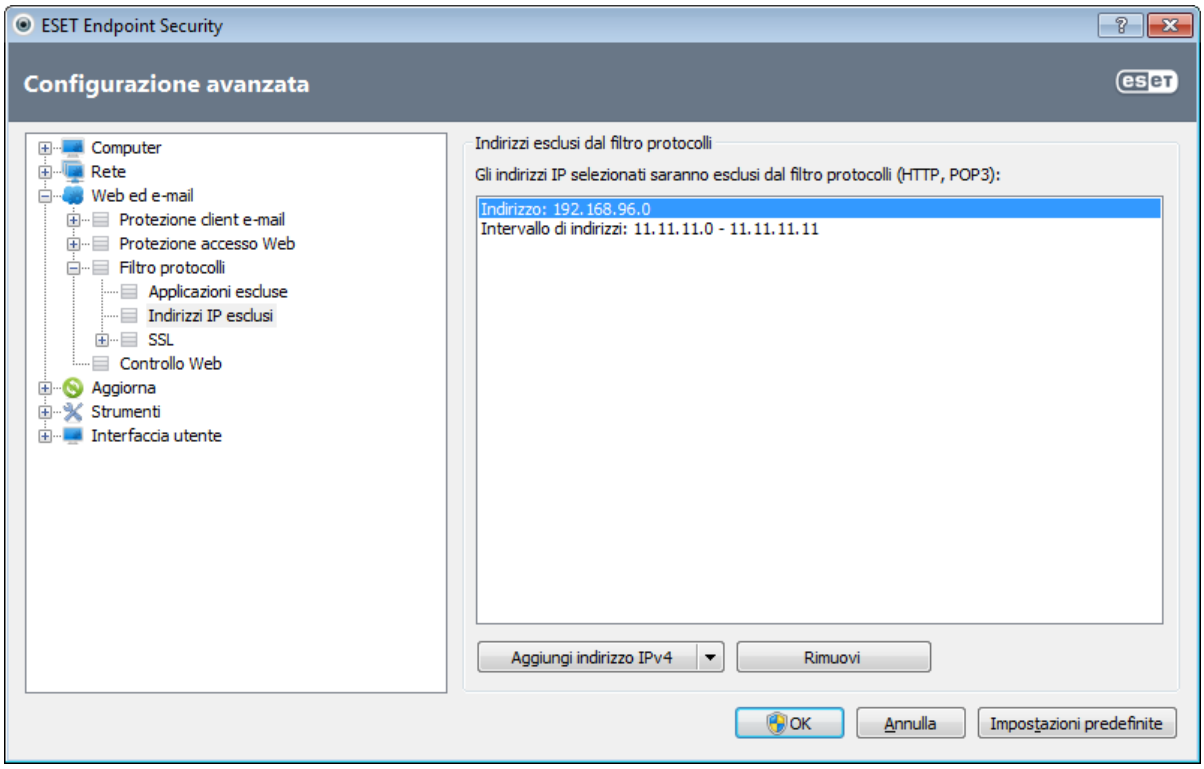


4.3.4.3 Indirizzi IP esclusi

Le voci nell'elenco indirizzi saranno escluse dal filtro del contenuto del protocollo. Sulla comunicazione HTTP/POP3/IMAP da/verso gli indirizzi selezionati non verrà eseguito il rilevamento delle minacce. È consigliabile utilizzare questa opzione solo per gli indirizzi ritenuti affidabili.

Aggiungi indirizzo IPv4/IPv6 - Questa opzione consente di aggiungere un indirizzo IP/intervallo di indirizzi/subnet di un punto remoto a cui deve essere applicata la regola.

Rimuovi - Rimuove dall'elenco le voci selezionate.



4.3.4.3.1 Aggiungi indirizzo IPv4

Questa opzione consente di aggiungere un indirizzo IP/intervallo di indirizzi/subnet di un punto remoto a cui deve essere applicata la regola. Il protocollo Internet versione 4 è la versione meno recente, ma è ancora quello più utilizzato.

Indirizzo singolo - Aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola, ad esempio 192.168.0.10.

Intervallo di indirizzi - Immettere il primo e l'ultimo indirizzo IP per specificare l'intervallo IP (di più computer) per cui deve essere applicata la regola, ad esempio da 192.168.0.1 a 192.168.0.99.

Subnet - Subnet (gruppo di computer) definita da un indirizzo IP e da una maschera.

Ad esempio, 255.255.255.0 è la maschera di rete per il prefisso 192.168.1.0/24, che indica l'intervallo di indirizzi compreso tra 192.168.1.1 e 192.168.1.254.

4.3.4.3.2 Aggiungi indirizzo IPv6

Questa opzione consente di aggiungere un indirizzo IP/subnet di un punto remoto a cui deve essere applicata la regola. Si tratta della versione più recente del protocollo Internet e sostituirà la versione precedente 4.

Indirizzo singolo - Aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola, ad esempio 2001:718:1c01:16:214:22ff:fec9:ca5.

Subnet - Subnet (gruppo di computer) definita da un indirizzo IP e da una maschera, ad esempio 2002:c0a8:6301:1::1/64).

4.3.4.4 Verifica protocollo SSL

ESET Endpoint Security consente di verificare i protocolli incapsulati nel protocollo SSL. È possibile utilizzare varie modalità di scansione per le comunicazioni protette mediante il protocollo SSL utilizzando certificati attendibili, certificati sconosciuti o certificati che sono esclusi dalla verifica delle comunicazioni protette mediante il protocollo SSL.

Effettua sempre la scansione del protocollo SSL - Selezionare questa opzione per verificare tutte le comunicazioni protette mediante il protocollo SSL ad eccezione delle comunicazioni protette mediante i certificati esclusi dalla verifica. Se viene stabilita una nuova comunicazione usando un certificato firmato sconosciuto, all'utente non verrà inviata alcuna notifica e la comunicazione verrà filtrata in modo automatico. Quando si accede a un server con un certificato non attendibile contrassegnato dall'utente come attendibile (ovvero aggiunto all'elenco dei certificati attendibili), la comunicazione con il server è consentita e il contenuto del canale di comunicazione viene filtrato.

Chiedi conferma sui siti non visitati (possono essere impostate esclusioni) - Se si accede a un nuovo sito protetto SSL (con un certificato sconosciuto), verrà visualizzata una finestra di dialogo in cui è possibile scegliere l'azione da eseguire. Questa modalità consente di creare un elenco di certificati SSL che verranno esclusi dalla scansione.

Non controllare il protocollo SSL - Se viene selezionata questa opzione, il programma non eseguirà la scansione delle comunicazioni su SSL.

Applica le eccezioni create in base ai certificati - Consente di attivare l'utilizzo delle esclusioni specificate nei certificati attendibili ed esclusi per la scansione della comunicazione SSL. Questa opzione è disponibile se si seleziona **Effettua sempre la scansione del protocollo SSL**.

Blocca le comunicazioni crittografate che utilizzano il protocollo obsoleto SSL v2 - La comunicazione che utilizza la versione precedente del protocollo SSL verrà automaticamente bloccata.

4.3.4.4.1 Certificati

Affinché le comunicazioni SSL funzionino in modo adeguato nei browser/client e-mail, è fondamentale che il certificato radice per ESET, spol s r.o. sia aggiunto all'elenco dei certificati radice noti (autori). È pertanto necessario selezionare l'opzione **Aggiungi il certificato radice ai browser conosciuti**. Selezionare questa opzione per aggiungere automaticamente il certificato radice di ESET ai browser conosciuti (ad esempio, Opera, Firefox). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente (ad esempio, Internet Explorer). Per applicare il certificato a browser non supportati, fare clic su **Visualizza certificato** > **Dettagli** > **Copia su file...**, quindi importarlo manualmente nel browser.

In alcuni casi non è possibile verificare la validità del certificato mediante l'archivio Autorità di certificazione radice attendibili (ad esempio VeriSign). Ciò significa che il certificato è auto-firmato da qualcuno (ad esempio, l'amministratore di un server Web o una piccola azienda) e considerare questo certificato come attendibile non rappresenta sempre un rischio per la sicurezza. Gran parte delle aziende di grandi dimensioni, ad esempio le banche, utilizza certificati firmati da TRCA. Se è selezionata l'opzione **Chiedi conferma della validità dei certificati** (opzione predefinita), all'utente verrà richiesto di selezionare un'azione da eseguire quando si stabilisce una comunicazione crittografata. Verrà visualizzata una finestra di dialogo che consente di scegliere se contrassegnare il certificato come attendibile o se escluderlo. Nel caso in cui il certificato non sia presente nell'elenco TRCA, la finestra sarà rossa. In caso contrario, sarà di colore verde.

È possibile selezionare l'opzione **Blocca la comunicazione che utilizza il certificato** per terminare sempre una connessione crittografata al sito che utilizza il certificato non verificato.

Se il certificato non è valido oppure è danneggiato, significa che è scaduto o che l'auto-firma era errata. In questo caso, è consigliabile bloccare la comunicazione che utilizza il certificato.

4.3.4.4.1.1 Certificati attendibili

In aggiunta all'Archivio Autorità di certificazione radice attendibili integrato dove ESET Endpoint Security archivia i certificati attendibili, è possibile creare un elenco personalizzato di certificati attendibili che possono essere visualizzati in **Configurazione avanzata** (F5) > **Web ed e-mail** > **Filtro protocolli** > **SSL** > **Certificati** > **Certificati attendibili**. ESET Endpoint Security verificherà il contenuto delle comunicazioni crittografate che utilizzano i certificati presenti nell'elenco.

Per eliminare dall'elenco le voci selezionate, fare clic sul pulsante **Rimuovi**. Fare clic sull'opzione **Mostra** (o fare doppio clic sul certificato) per visualizzare le informazioni sul certificato selezionato.

4.3.4.4.1.2 Certificati esclusi

La sezione Certificati esclusi contiene i certificati ritenuti sicuri. Il contenuto delle comunicazioni crittografate che utilizzano i certificati nell'elenco non verrà verificato alla ricerca di minacce. È consigliabile escludere solo i certificati Web che sono garantiti come sicuri. In questo caso, non è necessario verificare la comunicazione che utilizza tali certificati. Per eliminare dall'elenco le voci selezionate, fare clic sul pulsante **Rimuovi**. Fare clic sull'opzione **Mostra** (o fare doppio clic sul certificato) per visualizzare le informazioni sul certificato selezionato.

4.3.4.4.1.3 Comunicazioni SSL crittografate

Se il computer è configurato per la scansione del protocollo SSL, potrebbe essere visualizzata una finestra di dialogo mediante la quale viene chiesto di scegliere un'azione da eseguire quando si tenta di stabilire una connessione crittografata (usando un certificato sconosciuto). La finestra di dialogo contiene le seguenti informazioni: nome dell'applicazione che ha avviato la comunicazione e del certificato utilizzato.

ESET Endpoint Security
Comunicazioni SSL crittografate
Certificato attendibile
Un'applicazione in esecuzione in questo computer tenta di comunicare su un canale SSL crittografato. Se si desidera controllare il contenuto del canale crittografato, contrassegnare il certificato come attendibile. Considerare il certificato del computer remoto come attendibile?
Applicazione: Google Chrome
Certificato: *.google.com
Sì
Sì, sempre
No
Escludi

Se non si trova nell'Archivio Autorità di certificazione radice attendibili, il certificato è considerato non attendibile.

ESET Endpoint Security
Comunicazioni SSL crittografate
Certificato non attendibile
Un'applicazione in esecuzione in questo computer tenta di comunicare su un canale SSL crittografato. Se si desidera controllare il contenuto del canale crittografato, contrassegnare il certificato come attendibile. Considerare il certificato del computer remoto come attendibile?
Applicazione: Google Chrome
Certificato:
Sì
Sì, sempre
No
Escludi

Per i certificati sono disponibili le azioni seguenti:

Sì - Il certificato verrà temporaneamente contrassegnato come attendibile per la sessione corrente e la finestra di avviso non verrà visualizzata al successivo tentativo di utilizzare il certificato.

Sì, sempre - Contrassegna il certificato come attendibile e lo aggiunge all'elenco dei certificati attendibili. Per i certificati attendibili non verrà visualizzata alcuna finestra di avviso.

No - Contrassegna il certificato come non attendibile per la sessione corrente. La finestra di avviso verrà visualizzata al successivo tentativo di utilizzo del certificato.

Escludi - Aggiunge il certificato all'elenco dei certificati esclusi. I dati trasferiti sul canale crittografato fornito non verranno controllati.

4.4 Controllo Web

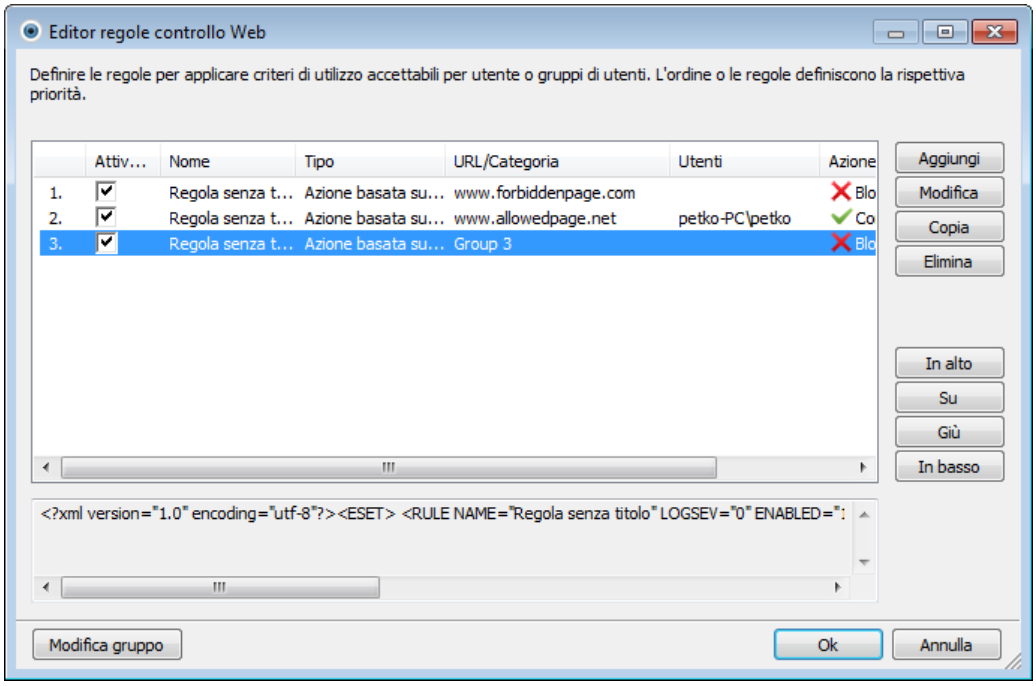
La sezione Controllo Web consente di configurare impostazioni che prevengono rischi di responsabilità legale per l'azienda. Include i siti Web che violano i diritti della proprietà intellettuale. Lo scopo è quello di impedire ai dipendenti di accedere a pagine contenenti contenuti inappropriati o dannosi o pagine che potrebbero avere un impatto negativo sulla produttività lavorativa.

Controllo Web consente di bloccare le pagine Web che possono contenere materiale potenzialmente inappropriato. Gli datori di lavoro o amministratori di sistema possono inoltre vietare l'accesso fino a più di 27 categorie di siti Web predefinite e più di 140 sottocategorie.

Le opzioni di configurazione del Controllo Web possono essere modificate in **Configurazione avanzata** (F5) > **Controllo Web**. La casella di controllo accanto a **Integrazione nel sistema** consente di integrare il Controllo Web in ESET Endpoint Security e attivare **Configura regole...** per accedere alla finestra Editor regole controllo Web.

4.4.1 Regole del controllo Web

Nella finestra **Editor regole controllo Web** sono visualizzate le regole esistenti per gli indirizzi URL e le categorie di pagine Web.



L'elenco delle regole contiene diverse descrizioni di una regola quali nome, tipo di blocco, azione da eseguire quando viene rilevata una corrispondenza con la regola del controllo Web e gravità del rapporto.

Fare clic su **Aggiungi** oppure su **Modifica** per gestire una regola. Fare clic su **Copia** per creare una nuova regola con le opzioni predefinite utilizzate per un'altra regola selezionata. Le stringhe XML visualizzate quando si seleziona una regola possono essere copiate negli Appunti in modo da essere utili agli amministratori di sistema per esportare/importare questi dati e utilizzarli, ad esempio in ESET Remote Administrator.

Premere CTRL e fare clic per selezionare più regole e applicare azioni a tutte le regole selezionate, ad esempio per eliminarle o spostarle in alto o in basso nell'elenco. Selezionare la casella di controllo **Attivata** per disattivare o attivare una regola. Questa opzione è utile se non si desidera eliminare definitivamente la regola in modo da poterla utilizzare in futuro.

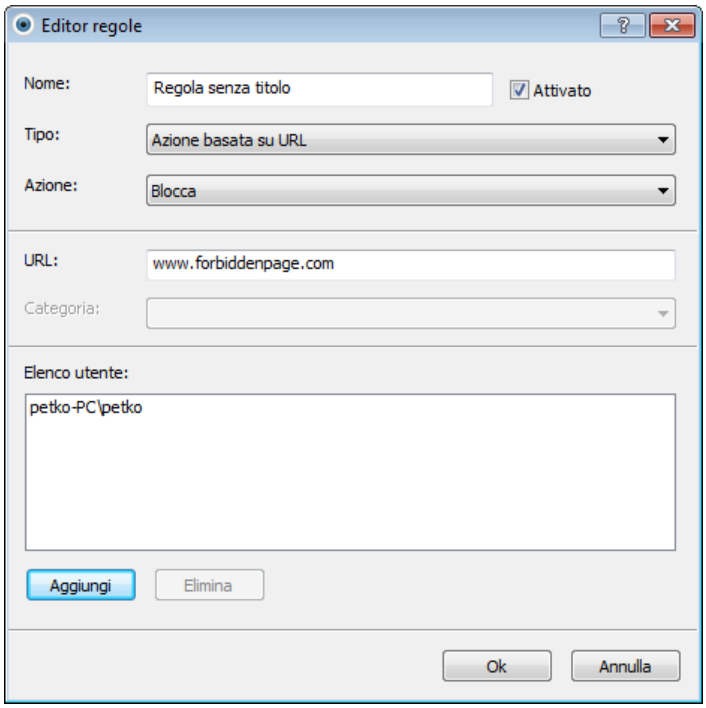
Il controllo viene eseguito mediante regole che sono classificate in base al rispettivo ordine di priorità, a partire dalle regole con priorità più alta.

Fare clic con il pulsante destro del mouse su una regola per visualizzare il menu contestuale. Qui è possibile impostare il livello di dettaglio (gravità) delle voci di rapporto di una regola. Le voci del rapporto possono essere visualizzate nella finestra principale di ESET Endpoint Security in **Strumenti** > **File di rapporto**.

Fare clic su **Modifica gruppo** per aprire la finestra Editor gruppi che consente di aggiungere o rimuovere le categorie e sottocategorie predefinite che appartengono a un gruppo corrispondente.

4.4.2 Aggiunta di regole del controllo Web

La finestra Regole del controllo Web consente di creare o modificare manualmente la regola di filtraggio esistente del controllo Web.



Immettere una descrizione della regola nel campo **Nome** per una più facile identificazione. Selezionare la casella di controllo **Attivata** per disattivare o attivare la regola. Questa opzione è utile se non si desidera eliminare definitivamente la regola.

Tipo di azione

- **Azione basata su URL** - Accedere al sito Web specificato. Immettere l'indirizzo URL appropriato nel campo **URL**.
- **Azione basata su categoria** - Dopo aver selezionato questa opzione, è necessario scegliere una categoria nel menu a discesa **Categoria**.

Nell'elenco degli indirizzi URL non è possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). Ad esempio, gli indirizzi delle pagine Web con più TLD devono essere inseriti manualmente (paginadiesempio.com, paginadiesempio.sk e così via). Quando si immette un dominio all'elenco, tutti i contenuti in tale dominio e in tutti i sottodomini (ad esempio sub.paginadiesempio.com) saranno bloccati o consentiti in base all'azione basata su URL scelta dall'utente.

Azione

- **Consenti** - L'accesso all'indirizzo URL/categoria sarà consentito.
- **Blocca** - L' indirizzo URL/categoria verrà bloccato.

Elenco utente

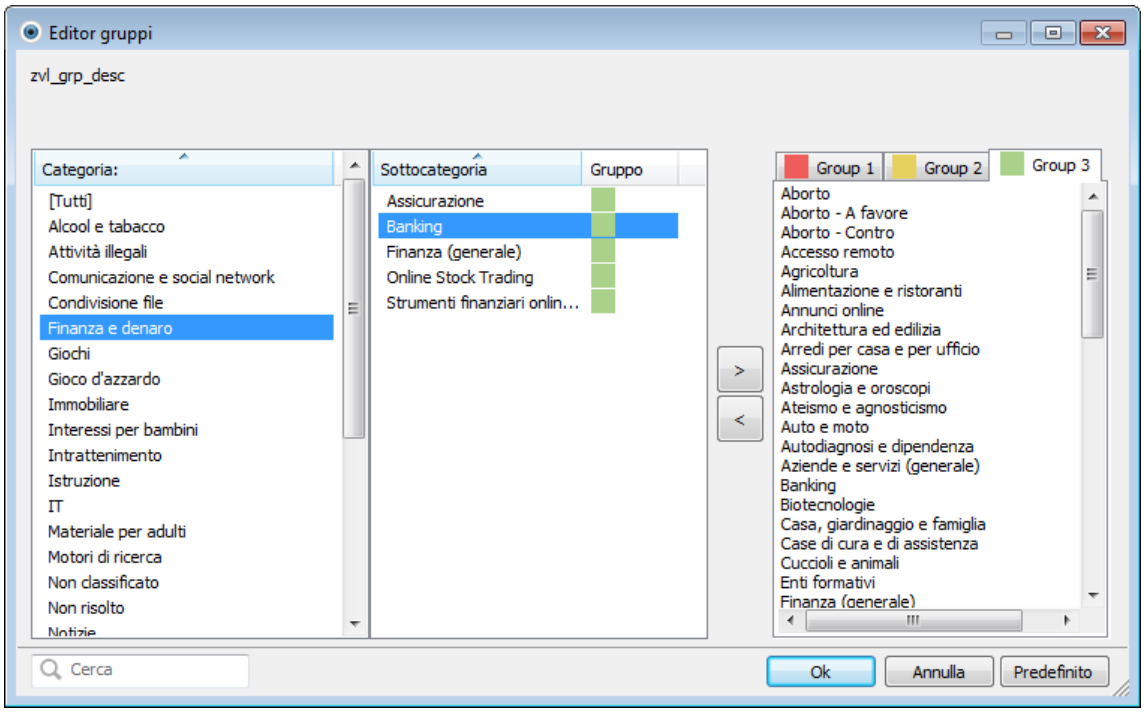
- **Aggiungi** - Visualizza la finestra di dialogo **Tipo di oggetto: Utenti o Gruppi** che consente di selezionare gli utenti desiderati.
- **Elimina** - Rimuove l'utente selezionato dal filtro.

4.4.3 Editor gruppi

La finestra Editor gruppi è suddivisa in due parti. Nella parte a destra è visualizzato un elenco di categorie e sottocategorie. Selezionare una categoria nell'elenco **Categoria** per visualizzare le rispettive sottocategorie. Gran parte delle sottocategorie appartiene a un gruppo contrassegnato con un colore.

Un gruppo di colore rosso contiene sottocategorie per adulti e/o con contenuti generalmente inappropriati. Un gruppo di colore verde comprende invece categorie di pagine Web che possono essere considerate accettabili.

Usare le frecce per aggiungere o rimuovere una sottocategoria selezionata a un gruppo selezionato.



Nota: una sottocategoria può appartenere a un solo gruppo. Alcune sottocategorie non sono incluse nei gruppi predefiniti, ad esempio Giochi. Per trovare una corrispondenza usando il filtro controllo Web, aggiungerla a un gruppo desiderato. Se la sottocategoria che si desidera aggiungere è già inclusa in un altro gruppo, verrà rimossa e aggiunta al gruppo selezionato.

Per ricercare un gruppo, immettere i termini di ricerca nel campo **Cerca** nell'angolo in basso a sinistra della finestra.

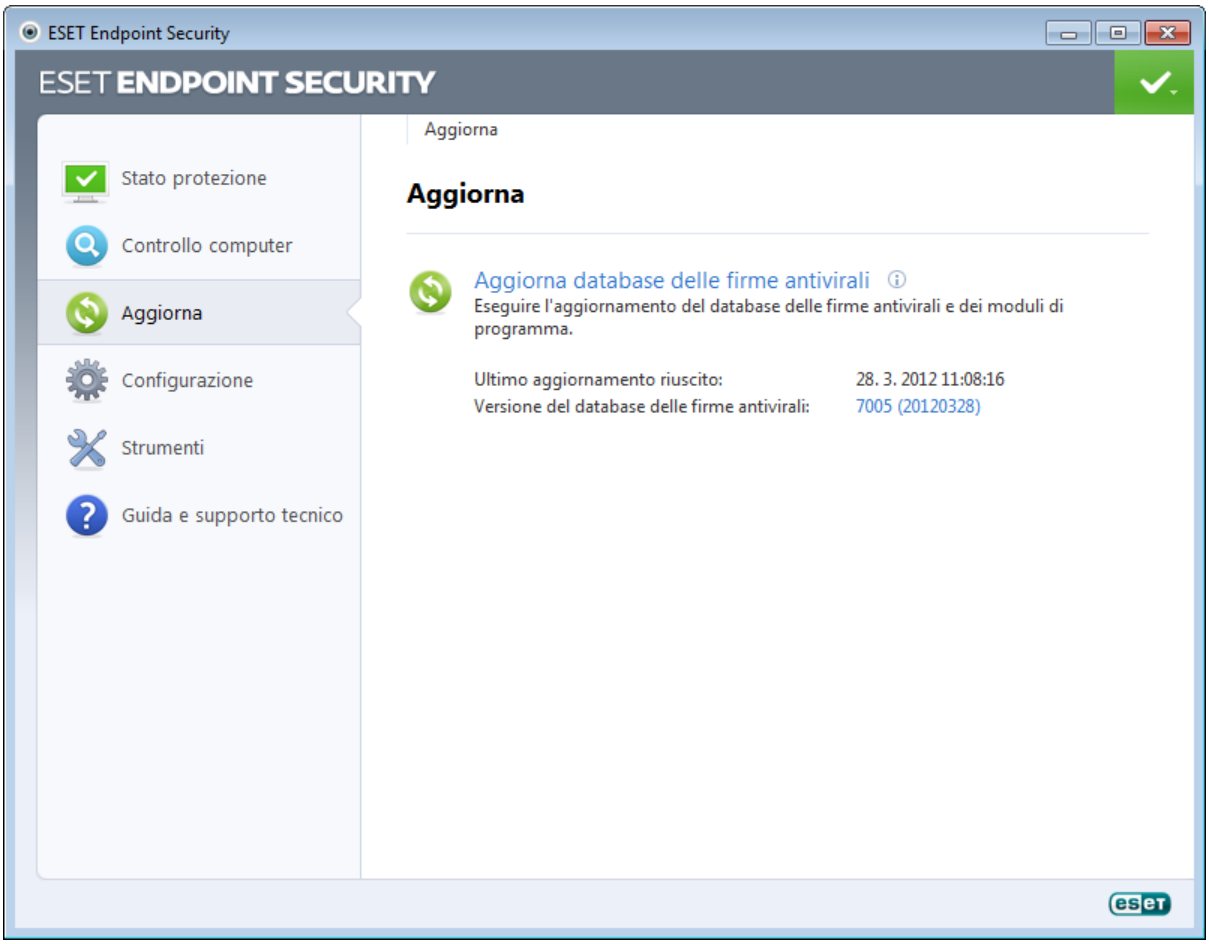
4.5 Aggiornamento del programma

L'aggiornamento periodico di ESET Endpoint Security rappresenta il miglior metodo per ottenere il livello massimo di protezione del computer. Il modulo di aggiornamento garantisce in due modi che il programma sia sempre aggiornato: attraverso l'aggiornamento rispettivamente del database delle firme antivirali e dei componenti del sistema.

Facendo clic su **Aggiorna** nella finestra principale del programma, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente e valutare se sia necessario un aggiornamento. Nella finestra principale sono inoltre contenute informazioni sulla versione del database delle firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito Web di ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

È inoltre disponibile l'opzione per avviare manualmente il processo di aggiornamento: **Aggiorna database delle firme antivirali**. L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi. È opportuno prestare particolare attenzione alla relativa configurazione e al funzionamento. Se durante l'installazione non si inseriscono informazioni sulla Licenza (nome utente e password), è possibile inserire il nome utente e la password durante l'aggiornamento per accedere ai server di aggiornamento ESET.

NOTA: il nome utente e la password vengono forniti da ESET dopo l'acquisto di ESET Endpoint Security.

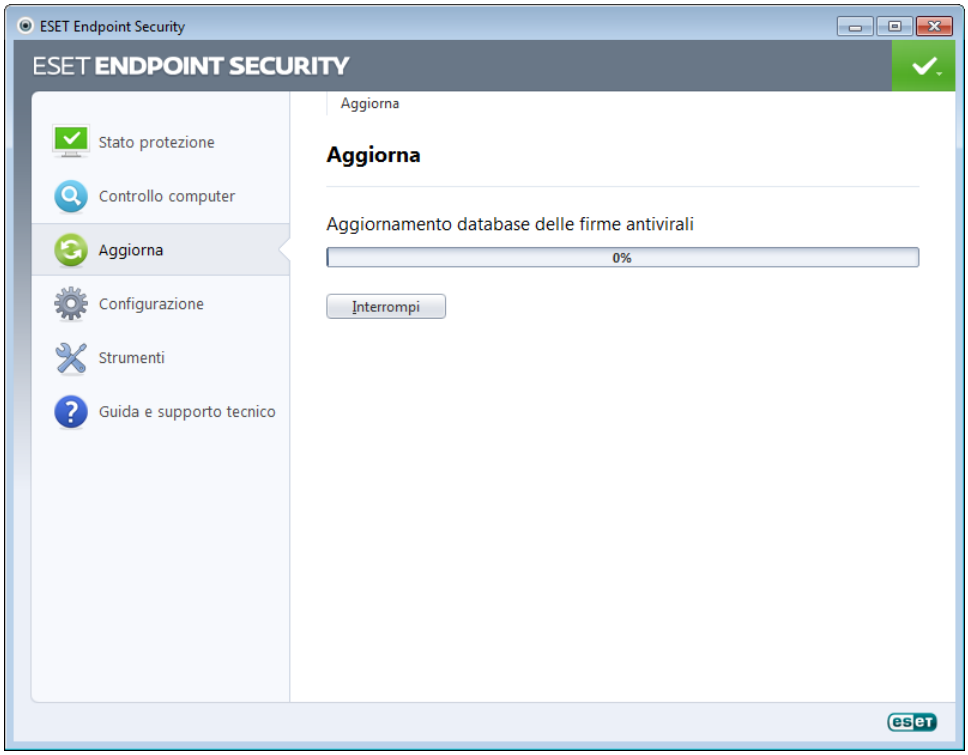


Ultimo aggiornamento riuscito - Data dell'ultimo aggiornamento. Accertarsi che la data sia recente: significa che il database delle firme antivirali è aggiornato.

Versione del database delle firme antivirali - Numero del database delle firme antivirali, ma anche collegamento attivo al sito Web di ESET. Selezionare per visualizzare un elenco di tutte le firme aggiunte in un aggiornamento specifico.

Processo di aggiornamento

Dopo aver selezionato **Aggiornamento del database delle firme antivirali**, viene avviato il processo di download. Verranno visualizzati una barra di avanzamento del download e il tempo rimanente per il completamento dell'operazione. Per interrompere l'aggiornamento, fare clic su **Interrompi**.

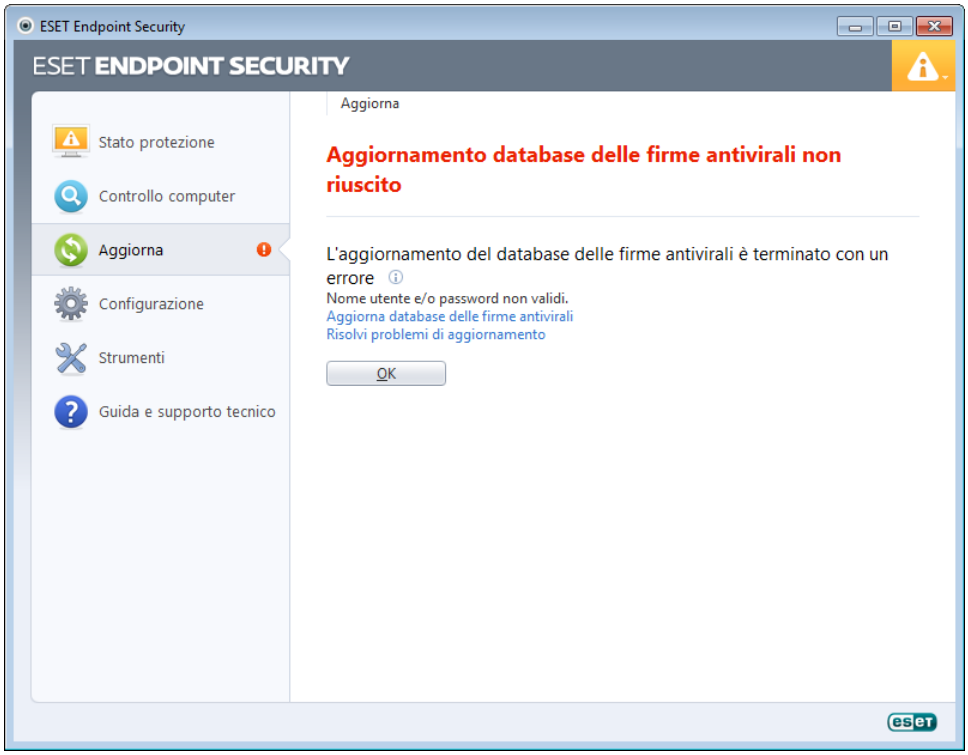


Importante: in circostanze normali, quando gli aggiornamenti sono scaricati correttamente, nella finestra **Aggiornamento** viene visualizzato il messaggio **Aggiornamento non necessario. Il database delle firme antivirali è aggiornato**. In caso contrario, il programma è obsoleto ed è maggiormente esposto alle infezioni. Aggiornare il database delle firme antivirali appena possibile. In caso contrario, viene visualizzato uno dei seguenti messaggi:

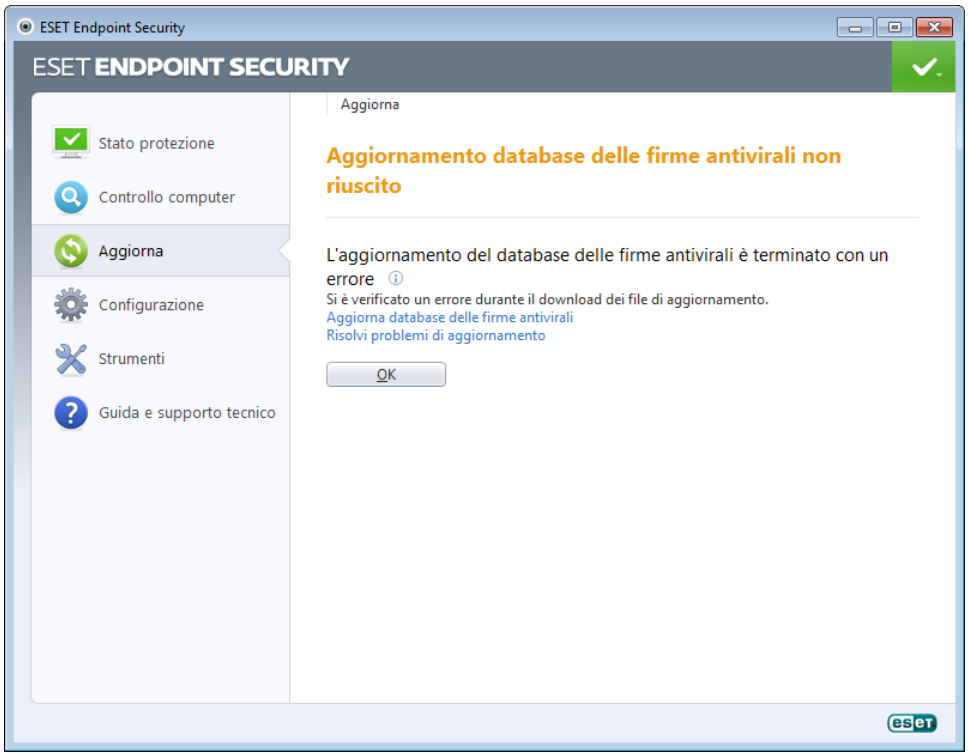
Il database delle firme antivirali è obsoleto - Questo errore viene visualizzato dopo diversi tentativi non riusciti di aggiornare il database delle firme antivirali. Si consiglia di controllare le impostazioni dell'aggiornamento. Spesso questo errore viene visualizzato perché i dati di autenticazione non vengono immessi correttamente o le impostazioni di connessione sono errate.

Il messaggio di notifica precedente è correlato ai due messaggi che seguono, relativi ad aggiornamenti non riusciti (**Aggiornamento del database delle firme antivirali non riuscito**) :

1. **Nome utente e/o password non validi** - Il nome utente e la password non sono stati inseriti correttamente nella configurazione dell'aggiornamento. Si consiglia di verificare i propri dati di autenticazione. Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi selezionare **Accedi a configurazione avanzata...** oppure premere F5 sulla tastiera) sono disponibili ulteriori opzioni di aggiornamento. Fare clic su **Aggiorna** > **Generale** nella struttura Configurazione avanzata per inserire un nuovo nome utente e una nuova password.



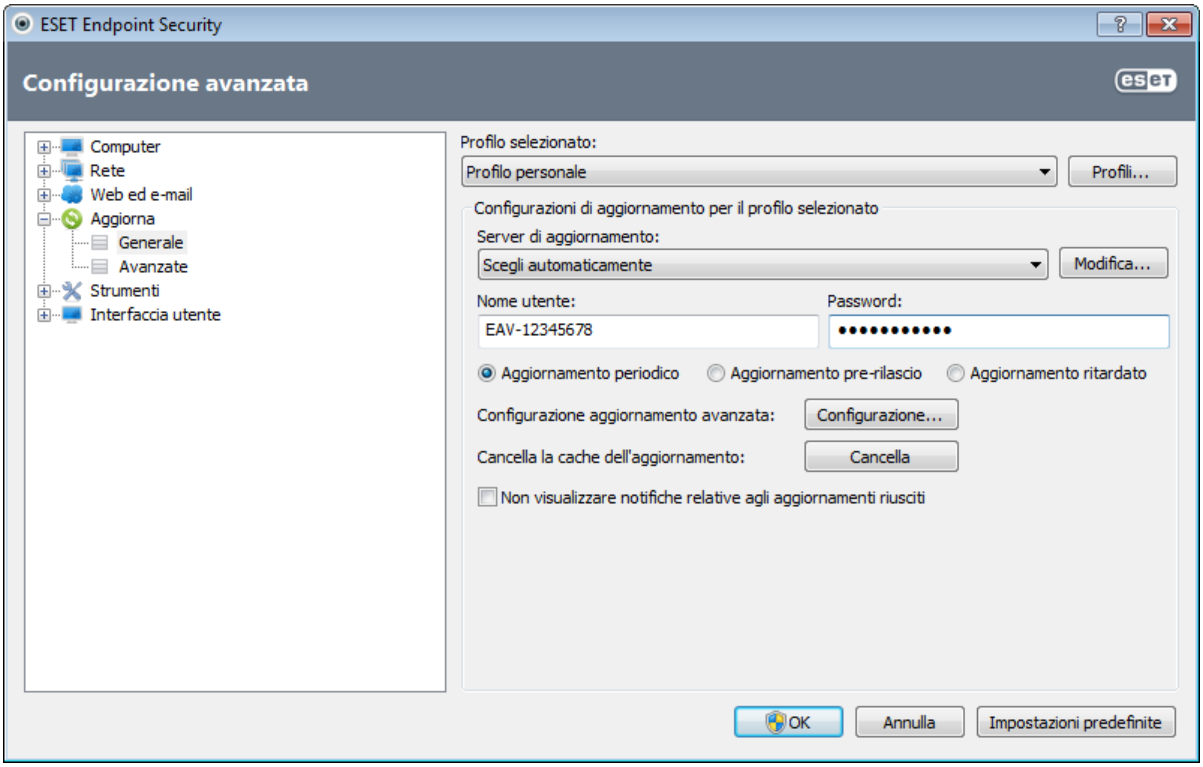
2. **Si è verificato un errore durante il download dei file di aggiornamento** - L'errore potrebbe essere causato da Impostazioni di connessione Internet non corrette. Si consiglia di verificare la connettività Internet (aprendo un qualsiasi sito Web nel browser). Se il sito Web non si apre, è possibile che la connessione Internet non sia presente o che si siano verificati problemi di connettività nel computer in uso. Se la connessione Internet non è attiva, contattare il proprio Provider di servizi Internet (ISP).



4.5.1 Configurazione dell'aggiornamento

Le opzioni di configurazione dell'aggiornamento sono disponibili nella struttura **Configurazione avanzata** (tasto F5), facendo clic su **Aggiorna** > **Generale**. Questa sezione consente di specificare informazioni sull'origine dell'aggiornamento, come ad esempio i server di aggiornamento e i dati per l'autenticazione di tali server. Per impostazione predefinita, il menu a discesa **Server di aggiornamento** è impostato su **Scegli automaticamente** per garantire che i file di aggiornamento vengano scaricati automaticamente dal server ESET con meno traffico di rete.

Affinché gli aggiornamenti vengano scaricati correttamente, occorre configurare tutti i parametri necessari. Se si utilizza un firewall, assicurarsi che al programma sia consentito comunicare con Internet (ad es., comunicazione HTTP).



Il profilo di aggiornamento attualmente in uso viene visualizzato nel menu a discesa **Profilo selezionato**. Per creare un nuovo profilo, fare clic su **Profili...**.

L'elenco dei server di aggiornamento disponibili è accessibile tramite il menu a discesa **Server di aggiornamento**. Il server di aggiornamento è la posizione di archiviazione degli aggiornamenti. Se si utilizza un server ESET, lasciare selezionata l'opzione predefinita **Scegli automaticamente**. Per aggiungere un nuovo server di aggiornamento, scegliere **Modifica...** nella sezione **Impostazioni di aggiornamento per il profilo selezionato**, quindi fare clic sul pulsante **Aggiungi**.

Quando si utilizza un server HTTP locale (noto anche come Mirror), il server di aggiornamento deve essere impostato come riportato di seguito:
http://nome_computer_o_relativo_indirizzo_IP:2221

Quando si utilizza un server HTTP locale usando SSL, il server di aggiornamento deve essere impostato come riportato di seguito:
https://nome_computer_o_relativo_indirizzo_IP:2221

L'autenticazione per i server di aggiornamento si basa sul **Nome utente** e sulla **Password** generati e inviati dopo aver acquistato il programma. Quando si utilizza un server Mirror locale, la verifica dipende dalla relativa configurazione. Per impostazione predefinita, non è richiesta alcuna verifica, pertanto i campi **Nome utente** e **Password** vengono lasciati vuoti.

Gli aggiornamenti pre-rilascio (opzione **Aggiornamento pre-rilascio**) sono aggiornamenti sottoposti ad approfondite verifiche interne e saranno a breve disponibili a livello globale. Gli aggiornamenti pre-rilascio consentono di accedere ai metodi di rilevamento e correzioni più recenti. È tuttavia probabile che tali aggiornamenti non siano sempre sufficientemente stabili e NON devono pertanto essere utilizzati su server di produzione e workstation dove è richiesta massima disponibilità e stabilità. L'elenco dei moduli correnti è disponibile in **Guida e supporto tecnico** > **Informazioni su ESET Endpoint Security**. È consigliabile lasciare attivata l'opzione **Aggiornamento periodico** selezionata per impostazione predefinita. Gli utenti Business possono selezionare l'opzione **Aggiornamento ritardato** per eseguire l'aggiornamento da server di aggiornamento speciali che mettono a disposizione nuove versioni dei database antivirus

con un ritardo di almeno X ore, ad esempio per testare i database in un ambiente reale e valutare quindi se sono stabili.

Selezionare il pulsante **Configurazione...** accanto a **Impostazione aggiornamento avanzata** per visualizzare una finestra contenente le opzioni di aggiornamento avanzate.

In caso di problemi di aggiornamento, fare clic sul pulsante **Cancella...** per svuotare la cartella dei file di aggiornamento temporanei.

Non visualizzare la notifica dopo il completamento dell'aggiornamento - Disattiva la notifica sulla barra delle applicazioni nell'angolo in basso a destra della schermata. È utile selezionare questa opzione se è in esecuzione un'applicazione a schermo intero o un videogioco. Tenere presente che se è attiva la Modalità Presentazione , tutte le notifiche saranno disattivate.

4.5.1.1 Aggiorna profili

Per varie configurazioni e attività di aggiornamento è possibile creare profili di aggiornamento. La creazione dei profili di aggiornamento è particolarmente utile per gli utenti mobili, i quali possono creare un profilo alternativo per le proprietà di connessione a Internet che cambiano periodicamente.

Nel menu a discesa **Profilo selezionato** è visualizzato il profilo correntemente selezionato, configurato per impostazione predefinita su **Profilo personale**. Per creare un nuovo profilo, fare clic sul pulsante **Profili...**, quindi selezionare il pulsante **Aggiungi...** e immettere il proprio **Nome profilo**. Quando si crea un nuovo profilo, è possibile copiare le impostazioni da uno esistente selezionandolo dal menu a discesa **Copia impostazioni dal profilo**.

Nella finestra di configurazione del profilo è possibile specificare il server di aggiornamento da un elenco di server disponibili oppure aggiungere un nuovo server. L'elenco dei server di aggiornamento esistenti è disponibile nel menu a discesa **Server di aggiornamento**. Per aggiungere un nuovo server di aggiornamento, scegliere **Modifica** nella sezione **Impostazioni di aggiornamento per il profilo selezionato**, quindi fare clic sul pulsante **Aggiungi**.

4.5.1.2 Configurazione aggiornamento avanzata

Per visualizzare l'Impostazione aggiornamento avanzata, fare clic sul pulsante **Configurazione...**. Le opzioni dell'impostazione aggiornamento avanzata includono la configurazione della **Modalità di aggiornamento**, **Proxy HTTP**, **LAN** e **Mirror**.

4.5.1.2.1 Modalità di aggiornamento

La scheda **Modalità di aggiornamento** contiene opzioni correlate all'aggiornamento dei componenti di programma. Il programma consente di preimpostare le azioni da eseguire quando è disponibile un nuovo aggiornamento dei componenti di programma.

Gli aggiornamenti dei componenti di programma aggiungono nuove funzioni o introducono modifiche alle funzioni già esistenti nelle versioni precedenti. Può essere eseguito automaticamente senza alcun intervento da parte dell'utente oppure è possibile scegliere di ricevere una notifica. Dopo che è stato installato l'aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer. Nella sezione **Aggiornamento componenti programma** sono disponibili tre opzioni:

- **Non aggiornare mai i componenti di programma** - L'aggiornamento dei componenti di programma non viene eseguito. Questa opzione è adatta alle installazioni su server, poiché di norma i server possono essere riavviati solo durante la manutenzione.
- **Aggiorna sempre i componenti di programma** - L'aggiornamento dei componenti di programma verrà scaricato e installato automaticamente. Ricordare che potrebbe essere necessario riavviare il computer.
- **Chiedi prima di scaricare i componenti di programma** - Opzione predefinita. All'utente verrà chiesto di confermare o rifiutare gli aggiornamenti dei componenti di programma, quando disponibili.

Dopo aver eseguito un aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer in modo da garantire il corretto funzionamento di tutti i moduli. La sezione **Riavvia dopo l'aggiornamento dei componenti di programma** consente di selezionare una delle opzioni seguenti:

- **Non riavviare mai il computer** - Non sarà richiesto di riavviare il computer, anche se è necessario. Questa opzione non è consigliata poiché il computer potrebbe non funzionare correttamente fino al riavvio successivo.
- **Proponi il riavvio del computer se necessario** - Opzione predefinita. Dopo l'aggiornamento dei componenti di programma verrà visualizzata una finestra di dialogo con la richiesta di riavviare il computer.
- **Se necessario, riavvia il computer senza notifica** - Dopo l'aggiornamento dei componenti di programma, il computer verrà riavviato (se necessario).

NOTA: la scelta dell'opzione più adatta dipende dalla workstation sulla quale saranno applicate le impostazioni. Tenere

presente che esistono alcune differenze tra le workstation e i server. Il riavvio automatico del server dopo un aggiornamento di un componente di programma potrebbe ad esempio causare gravi danni al sistema.

Se è selezionata l'opzione **Chiedi prima di scaricare l'aggiornamento**, verrà visualizzata una notifica ogni volta che è disponibile un nuovo aggiornamento.

Se la dimensione del file di aggiornamento supera il valore indicato nel campo **Chiedi se un file di aggiornamento è maggiore di**, verrà visualizzata una notifica.

4.5.1.2.2 Server proxy

Per accedere alle opzioni di configurazione del server proxy per un determinato profilo di aggiornamento, fare clic su **Aggiorna** nella struttura Configurazione avanzata (F5), quindi selezionare il pulsante **Configurazione...** a destra di **Configurazione aggiornamento avanzata**. Fare clic sulla scheda **Proxy HTTP** e selezionare una delle tre opzioni seguenti:

- **Utilizza impostazioni server proxy globali**
- **Non utilizzare server proxy**
- **Connessione tramite server proxy**

Se si seleziona l'opzione **Utilizza impostazioni server proxy globali**, verranno utilizzate le opzioni di configurazione del server proxy già specificate all'interno della sottostruttura **Strumenti** > **Server proxy** della struttura Configurazione avanzata.

Selezionare l'opzione **Non utilizzare server proxy** per specificare che non verrà utilizzato alcun server proxy per l'aggiornamento di ESET Endpoint Security.

Selezionare l'opzione **Connessione tramite server proxy** nei seguenti casi:

- È necessario utilizzare un server proxy per aggiornare ESET Endpoint Security e tale server proxy è differente da quello specificato nelle impostazioni globali (**Strumenti** > **Server proxy**). In questo caso, sarà necessario fornire alcune informazioni aggiuntive: Indirizzo del **Server proxy**, **Porta** di comunicazione e **Nome utente** e **Password** del server proxy, se richiesti.
- Le impostazioni del server proxy non sono state impostate a livello globale. ESET Endpoint Security si connetterà tuttavia a un server proxy per verificare la disponibilità di aggiornamenti.
- Il computer è connesso a Internet tramite un server proxy. Le impostazioni vengono estrapolate da Internet Explorer durante l'installazione del programma, ma se successivamente vengono modificate, ad esempio se si cambia il provider di servizi Internet (ISP), verificare che le impostazioni del proxy HTTP visualizzate in questa finestra siano corrette. In caso contrario, il programma non sarà in grado di connettersi ai server di aggiornamento.

L'impostazione predefinita per il server proxy è **Utilizza impostazioni server proxy globali**.

NOTA: i dati di autenticazione, ad esempio il **Nome utente** e **Password**, sono necessari per accedere al server proxy. Compilare questi campi solo se sono richiesti un nome utente e una password. Tenere presente che questi campi non costituiscono nome utente e password per ESET Endpoint Security e devono essere immessi solo se è necessaria una password per accedere a Internet mediante un server proxy.

4.5.1.2.3 Connessione alla LAN

Durante l'aggiornamento da un server locale con un sistema operativo basato su NT, per impostazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete. Nella maggior parte dei casi, un account di sistema locale non dispone di diritti di accesso sufficienti per la cartella Mirror (che contiene copie dei file di aggiornamento). In questo caso, immettere nome utente e password nella sezione di impostazione dell'aggiornamento o specificare un account esistente che il programma utilizzerà per accedere al server di aggiornamento (Mirror).

Per configurare tale account, fare clic sulla scheda **LAN**. Nella sezione **Connetti a LAN come** sono disponibili le opzioni **Account di sistema (predefinito)**, **Utente attuale** e **Utente specificato**.

Selezionare l'opzione **Account di sistema (predefinito)** per utilizzare l'account di sistema per l'autenticazione. In genere non viene eseguito alcun processo di autenticazione se nella sezione principale di impostazione dell'aggiornamento non sono specificati dati di autenticazione.

Per essere certi che il programma esegua l'autenticazione utilizzando l'account di un utente che ha eseguito correntemente l'accesso, selezionare **Utente attuale**. Lo svantaggio di questa soluzione consiste nel fatto che il programma non è in grado di connettersi al server di aggiornamento se nessun utente ha eseguito correntemente l'accesso.

Selezionare **Utente specificato** se si desidera che il programma utilizzi un account utente specifico per l'autenticazione.

Utilizzare questo metodo quando la connessione con l'account di sistema predefinito non riesce. Tenere presente che l'account dell'utente specificato deve disporre dell'accesso alla directory dei file di aggiornamento sul server locale. In caso contrario, il programma non sarà in grado di stabilire una connessione e scaricare gli aggiornamenti.

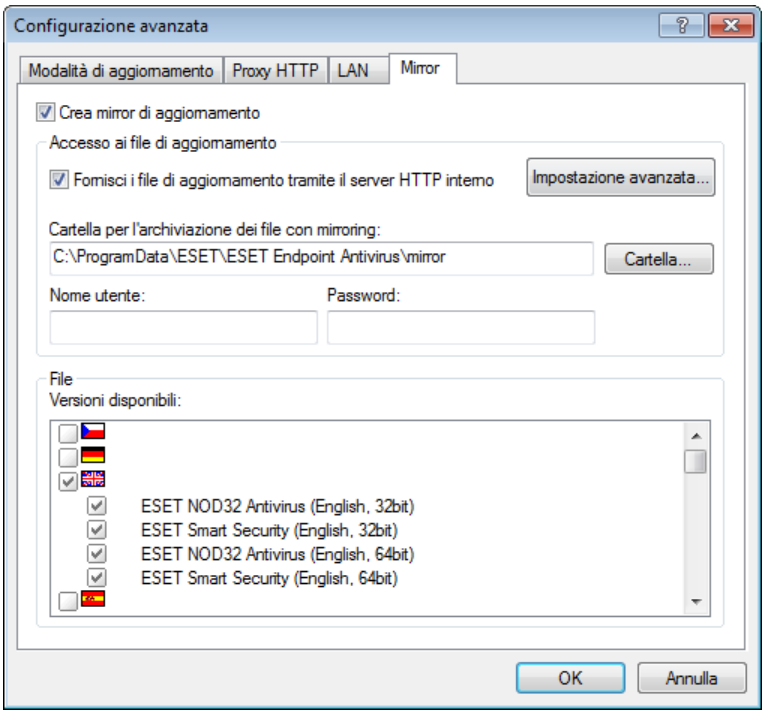
Avviso: Se si seleziona **Utente attuale** o **Utente specificato**, è possibile che si verifichi un errore quando si modifica l'identità del programma per l'utente desiderato. È consigliabile immettere i dati di autenticazione della LAN nella sezione principale di configurazione dell'aggiornamento. In questa sezione di impostazione dell'aggiornamento, i dati di autenticazione devono essere inseriti come segue: nome_dominio\utente (se si tratta di un gruppo di lavoro, immettere none_gruppodilavoro\nome) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

Selezionare l'opzione **Disconnetti dal server dopo l'aggiornamento** se la connessione al server rimane attiva anche dopo che sono stati scaricati gli aggiornamenti.

4.5.1.2.4 Creazione di copie di aggiornamento - Mirror

ESET Endpoint Security consente di creare copie di file di aggiornamento che è possibile utilizzare per aggiornare altre workstation della rete. Creazione del "mirror" - è utile disporre di una copia dei file di aggiornamento nell'ambiente della rete LAN poiché in questo modo i file di aggiornamento non devono essere scaricati ripetutamente dal server di aggiornamento del fornitore e da ogni singola workstation. Viene eseguito un download centralizzato sul server mirror locale, quindi i file vengono distribuiti a tutte le workstation, evitando il rischio di un potenziale sovraccarico del traffico di rete. L'aggiornamento delle workstation client da un Mirror consente di ottimizzare il bilanciamento del carico di rete e di risparmiare ampiezza di banda per la connessione a Internet.

Le opzioni di configurazione per il server Mirror locale sono accessibili (dopo aver aggiunto una chiave di licenza valida nella gestione licenze nella sezione Configurazione avanzata di ESET Endpoint Security) nella sezione di configurazione aggiornamento avanzata. Per accedere a questa sezione, premere F5 e fare clic su **Aggiorna** nella struttura Configurazione avanzata, quindi selezionare il pulsante **Configurazione...** accanto a **Configurazione aggiornamento avanzata** e selezionare la scheda **Mirror**.



Il primo passaggio della procedura di configurazione del Mirror consiste nel selezionare l'opzione **Crea mirror di aggiornamento**. Selezionando questa opzione vengono attivate altre opzioni di configurazione del Mirror come la modalità di accesso ai file di aggiornamento e il percorso di aggiornamento per i file con mirroring.

Fornire file di aggiornamento tramite il server HTTP interno - Se questa opzione è attivata, è possibile accedere ai file di aggiornamento tramite HTTP senza che vengano richiesti nome utente e password. Fare clic su Configurazione avanzata... per configurare le opzioni mirror avanzate.

Nota: su Windows XP, il server HTTP richiede il SP2 e successivi.

I metodi di attivazione del Mirroring sono descritti in dettaglio nella sezione Aggiornamento dal Mirror. Per il momento, tenere presente che sono disponibili due metodi di base per l'accesso al Mirror: la cartella con i file di aggiornamento può essere presentata come una cartella di rete condivisa o come un server HTTP.

La cartella dedicata alla memorizzazione dei file di aggiornamento per il Mirror è definita nella sezione **Cartella per l'archiviazione dei file con mirroring**. Fare clic su **Cartella...** per cercare una cartella sul computer locale o sulla cartella di rete condivisa. Se è necessaria l'autorizzazione per la cartella specificata, i dati di autenticazione devono essere immessi nei campi **Nome utente** e **Password**. Se la cartella di destinazione selezionata si trova su un disco di rete che esegue un sistema operativo Windows NT/2000/XP, il Nome utente e la Password specificati devono disporre privilegi di scrittura per la cartella selezionata. Nome utente e Password devono essere specificati nel formato Dominio/Utente o Gruppodilavoro/Utente. È necessario specificare le password corrispondenti.

Quando si configura il Mirror, è anche possibile specificare le versioni della lingua per le quali si desidera scaricare le copie di aggiornamento che sono attualmente supportate dal server di mirroring configurato dall'utente. L'impostazione della versione della lingua è disponibile nell'elenco **Versioni disponibili**.

4.5.1.2.4.1 Aggiornamento dal Mirror

Sono disponibili due metodi di base per la configurazione del mirror: la cartella con i file di aggiornamento può essere presentata come una cartella di rete condivisa o come un server HTTP.

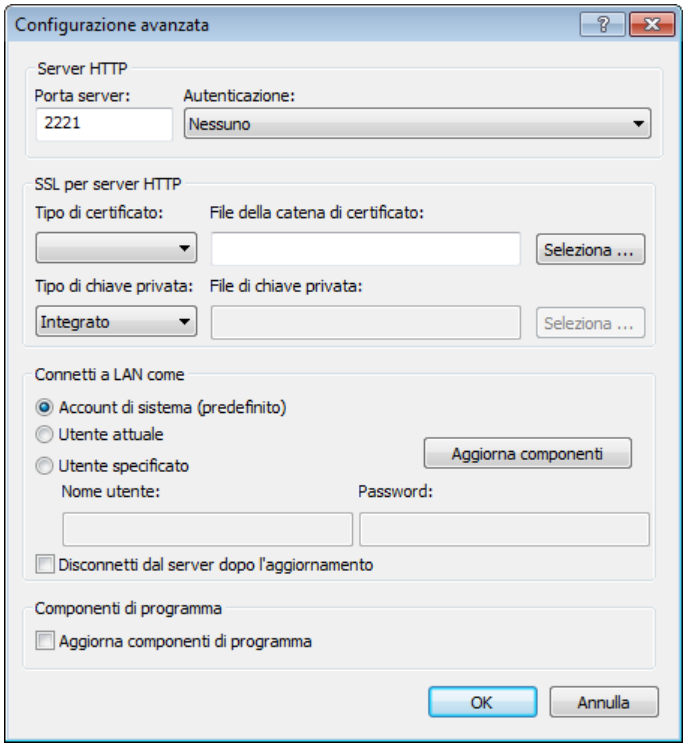
Accesso al Mirror mediante un server HTTP interno

Questa rappresenta la configurazione predefinita specificata nella configurazione originale del programma. Per consentire l'accesso al Mirror tramite il server HTTP, accedere alla sezione **Configurazione aggiornamento avanzata** (fare clic sulla scheda **Mirror**) e selezionare l'opzione **Crea mirror di aggiornamento**.

Nella sezione **Configurazione avanzata** della scheda **Mirror** è possibile specificare la **Porta server** di ascolto del server HTTP oltre al tipo di **Autenticazione** utilizzata dal server HTTP. Per impostazione predefinita, la porta server è configurata su **2221**. L'opzione **Autenticazione** definisce il metodo di autenticazione usato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **NESSUNO**, **Base** ed **NTLM**. Selezionare **Base** per utilizzare la codifica base64 con l'autenticazione di base di nome utente e password. L'opzione **NTLM** consente l'uso di un metodo di codifica sicuro. Per l'autenticazione, viene utilizzato l'utente creato sulla workstation di condivisione dei file di aggiornamento. L'impostazione predefinita è **NESSUNO**, che consente l'accesso ai file di aggiornamento senza che sia necessaria l'autenticazione.

Attenzione: se si desidera consentire l'accesso ai file di aggiornamento tramite il server HTTP, la cartella Mirror deve essere posizionata sullo stesso computer dell'istanza di ESET Endpoint Security che la crea.

Se si desidera eseguire il server HTTP con il supporto HTTPS (SSL), aggiungere il **File della catena di certificato** o generare un certificato autofirmato. Sono disponibili i tipi seguenti: **ASN**, **PEM** e **PFX**. È possibile scaricare i file di aggiornamento tramite il protocollo HTTPS che assicura maggiore protezione. Tramite questo protocollo è quasi impossibile tenere traccia dei trasferimenti di dati e delle credenziali di accesso. Per impostazione predefinita, l'opzione **Tipo di chiave privata** è configurata su **Integrata** (e, pertanto, per impostazione predefinita l'opzione **File di chiave privata** è disattivata), ovvero la chiave privata è un componente del file della catena di certificato selezionato.



Al termine della configurazione del Mirror, accedere alle workstation e aggiungere un nuovo server di aggiornamento. Per eseguire questa operazione, effettuare i seguenti passaggi:

- Aprire **Configurazione avanzata di ESET Endpoint Security** e fare clic su **Aggiorna** > **Generale**.
- Fare clic su **Modifica...** a destra del menu a discesa **Server di aggiornamento** e aggiungere un nuovo server usando uno dei formati seguenti:
  http://indirizzo_IP_del_server:2221
  https://indirizzo_IP_del_server:2221 (se è in uso SSL)
- Selezionare il server appena aggiunto dall'elenco di server di aggiornamento.

Accesso al Mirror tramite le condivisioni di sistema

È innanzitutto necessario creare una cartella condivisa su un dispositivo locale o di rete. Durante la creazione della cartella per il Mirror, è necessario garantire l'accesso "in scrittura" all'utente che salverà i file nella cartella e l'accesso "in lettura" a tutti gli utenti che aggiorneranno ESET Endpoint Security dalla cartella Mirror.

Configurare quindi l'accesso al Mirror nella sezione **Configurazione aggiornamento avanzata** della scheda **Mirror** disattivando l'opzione **Fornisci i file di aggiornamento tramite il server HTTP interno**. Questa opzione è attivata per impostazione predefinita nel pacchetto di installazione del programma.

Se la cartella condivisa è posizionata su un altro computer della rete, sarà necessario immettere i dati di autenticazione per l'accesso all'altro computer. Per inserire i dati di autenticazione, aprire **Configurazione avanzata** di ESET Endpoint Security (F5) e fare clic su **Aggiorna** > **Generale**. Fare clic sul pulsante **Configurazione...**, quindi selezionare la scheda **LAN**. Questa impostazione è la stessa anche per l'aggiornamento, come illustrato nella sezione Connessione alla LAN.

Una volta completata la configurazione del Mirror, accedere alle workstation e impostare \\UNC\PATH come server di aggiornamento. Questa operazione può essere completata effettuando i passaggi riportati di seguito:

- Aprire Configurazione avanzata di ESET Endpoint Security e selezionare **Aggiorna** > **Generale**.
- Fare clic su **Modifica...** accanto al server di aggiornamento e aggiungere un nuovo server usando il formato \\UNC\PATH.
- Selezionare il server appena aggiunto dall'elenco di server di aggiornamento.

NOTA: per un corretto funzionamento, il percorso alla cartella Mirror deve essere specificato come percorso UNC. Gli aggiornamenti dalle unità mappate potrebbero non funzionare.

L'ultima sezione controlla i componenti del programma (PCU). Per impostazione predefinita, i componenti del programma scaricati sono preparati per la copia sul mirror locale. Se la casella di controllo accanto a **Aggiorna componenti di programma** è selezionata, non è necessario fare clic su **Aggiorna componenti** poiché i file vengono copiati automaticamente sul mirror locale nel momento in cui sono disponibili. Per ulteriori informazioni sugli aggiornamenti dei componenti del programma, vedere Modalità di aggiornamento.

4.5.1.2.4.2 Risoluzione dei problemi di aggiornamento Mirror

Nella maggior parte dei casi, i problemi durante un aggiornamento da un server Mirror sono causati da uno o più dei seguenti motivi: specifica non corretta delle opzioni della cartella Mirror, autenticazione non corretta dei dati nella cartella Mirror, configurazione non corretta sulle workstation locali che tentano di scaricare i file di aggiornamento dal Mirror o una combinazione di questi motivi. Di seguito viene riportata una panoramica sui problemi più frequenti che potrebbero verificarsi durante un aggiornamento dal Mirror:

ESET Endpoint Security riporta un errore di connessione al server Mirror - Probabilmente causato da una specifica non corretta del server di aggiornamento (percorso di rete alla cartella Mirror) dal quale le workstation locali scaricano gli aggiornamenti. Per verificare la cartella, selezionare il menu **Start** di Windows, fare clic su **Esegui**, immettere il nome della cartella e selezionare **OK**. Dovrebbe essere visualizzato il contenuto della cartella.

ESET Endpoint Security richiede un nome utente e una password - Probabilmente causato dall'immissione non corretta dei dati di autenticazione (nome utente e password) nella sezione di aggiornamento.. Il nome utente e la password sono utilizzati per concedere l'accesso al server di aggiornamento dal quale il programma si aggiornerà. Verificare che i dati di autenticazione siano corretti e immessi nel formato appropriato. Ad esempio, Dominio/Nome utente o Gruppo di lavoro/Nome utente, oltre alle password corrispondenti. Se il server Mirror è accessibile a "Tutti", non significa l'accesso è concesso a qualsiasi utente. Con "Tutti" non si intendono utenti non autorizzati. Si intende solo che la cartella è accessibile a tutti gli utenti del dominio. Di conseguenza, se una cartella è accessibile a "Tutti", sarà comunque necessario specificare un nome utente di dominio e una password nella sezione di impostazione dell'aggiornamento.

ESET Endpoint Security riporta un errore di connessione al server Mirror - La comunicazione sulla porta definita per l'accesso alla versione HTTP del Mirror è bloccata.

4.5.1.3 Annullamento aggiornamento

Se si sospetta che un nuovo aggiornamento del database antivirus possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare qualsiasi aggiornamento per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati.

ESET Endpoint Security consente di eseguire il backup dei moduli e il ripristino (il cosiddetto annullamento) del database antivirus. Per creare snapshot del database antivirus, lasciare selezionata la casella di controllo **Crea snapshot dei file di aggiornamento**. Nel campo **Numero di snapshot memorizzati localmente** è definito il numero dei precedenti snapshot del database antivirus memorizzato nel file system del computer locale.

Se si seleziona **Annulla** (**Configurazione avanzata** (F5) > **Aggiorna** > **Avanzate**), è necessario scegliere un intervallo di tempo nel menu a discesa **Sospendi aggiornamenti** che indica il periodo di tempo nel quale gli aggiornamenti del database delle firme antivirali e del modulo di programma verranno sospesi.

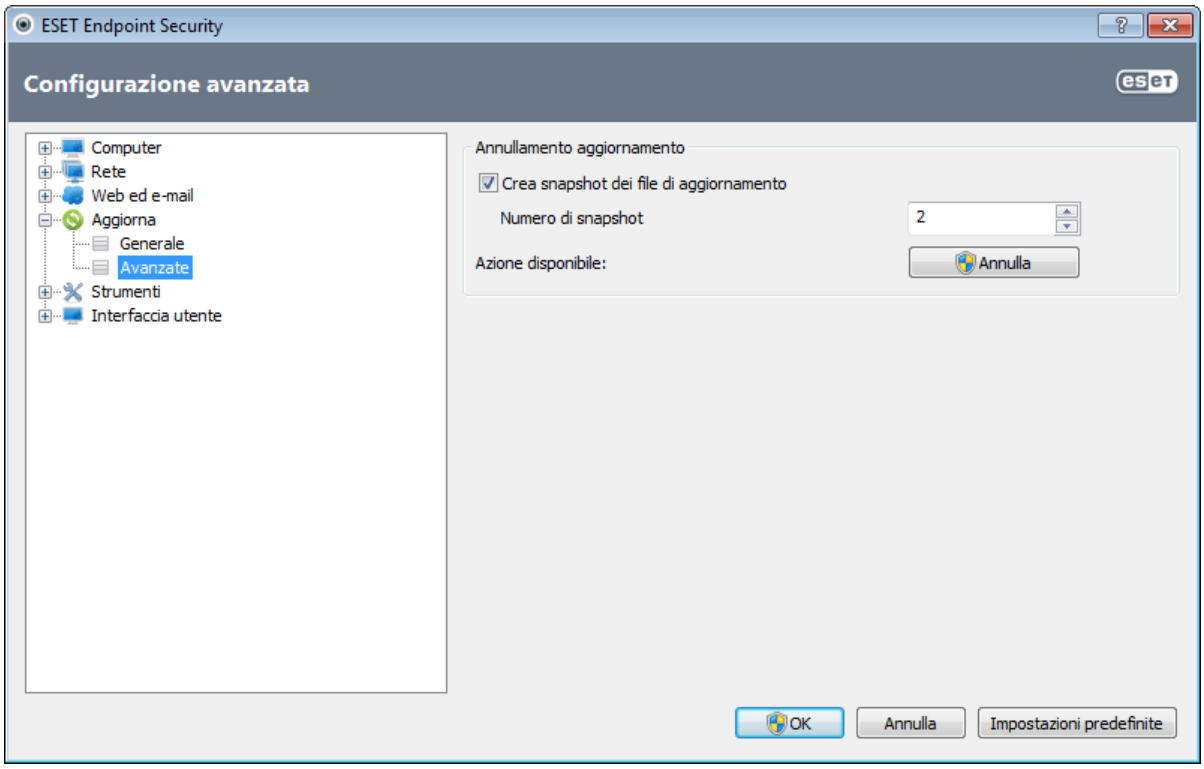
Annullamento file di aggiornamento
Sospendi aggiornamenti:
Per 48 ore
Se si conferma questa finestra di dialogo, il database antivirus e i moduli di programma verranno ripristinati sullo snapshot meno recente disponibile. Inoltre, gli aggiornamenti saranno sospesi per il periodo di tempo specificato o fino a quando verranno !ctls_updown32
OK
Annulla

Selezionare **Fino a revoca** se si desidera consentire l'esecuzione manuale periodica degli aggiornamenti. Non è consigliabile selezionare questa opzione in quanto rappresenta un potenziale rischio per la protezione.

Se è attivato un annullamento, il pulsante **Annulla** cambia in **Consenti aggiornamenti**. Non saranno consentiti aggiornamenti per l'intervallo di tempo selezionato nel menu a discesa Intervallo di tempo. La versione del database delle firme antivirali viene ripristinata alla versione più vecchia a disposizione e memorizzata come uno snapshot nel file system del computer locale.

Esempio: Si presupponga che la versione più recente del database delle firme antivirali corrisponda al numero 6871. Le versioni 6870 e 6868 sono memorizzate come snapshot del database delle firme antivirali. Si noti che la versione 6869 non è disponibile poiché, ad esempio, il computer è stato spento per un periodo di tempo prolungato. Se si inserisce 2 (due) nel campo **Numero di snapshot memorizzati localmente** e si seleziona **Annulla**, il database delle firme antivirali viene ripristinato al numero di versione 6868. L'operazione potrebbe richiedere alcuni minuti. Verificare se la versione del database delle firme antivirali è stata ripristinata a una versione precedente dalla finestra principale del programma di ESET Endpoint Security nella sezione Aggiornamento.

Le opzioni di configurazione per il server Mirror locale sono accessibili dopo aver aggiunto una chiave di licenza valida nella gestione licenze nella sezione Configurazione avanzata di ESET Endpoint Security. Se si utilizza la workstation come un mirror, è necessario che per le copie di aggiornamento sia stato accettato l'Accordo di Licenza per l'Utente finale (EULA) più recente prima che possano essere create come file di aggiornamento delle copie usati per aggiornare altre workstation presenti nella rete. Se durante l'aggiornamento è disponibile una versione più recente dell'EULA, verrà visualizzata una finestra di dialogo in cui viene richiesto all'utente di confermarla entro 60 secondi. Per eseguire questa operazione manualmente, fare clic su **Configura...** nella sezione **Licenze PCU** di questa finestra.



4.5.2 Come creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra principale visualizzata dopo aver selezionato l'opzione **Aggiorna** dal menu principale.

Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET Endpoint Security sono attivate le seguenti attività:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna delle attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, consultare la sezione Pianificazione attività.

4.6 Strumenti

Il menu **Strumenti** include moduli che consentono di semplificare l'amministrazione del programma e che offrono opzioni supplementari per gli utenti esperti.

Questo menu contiene i seguenti strumenti:

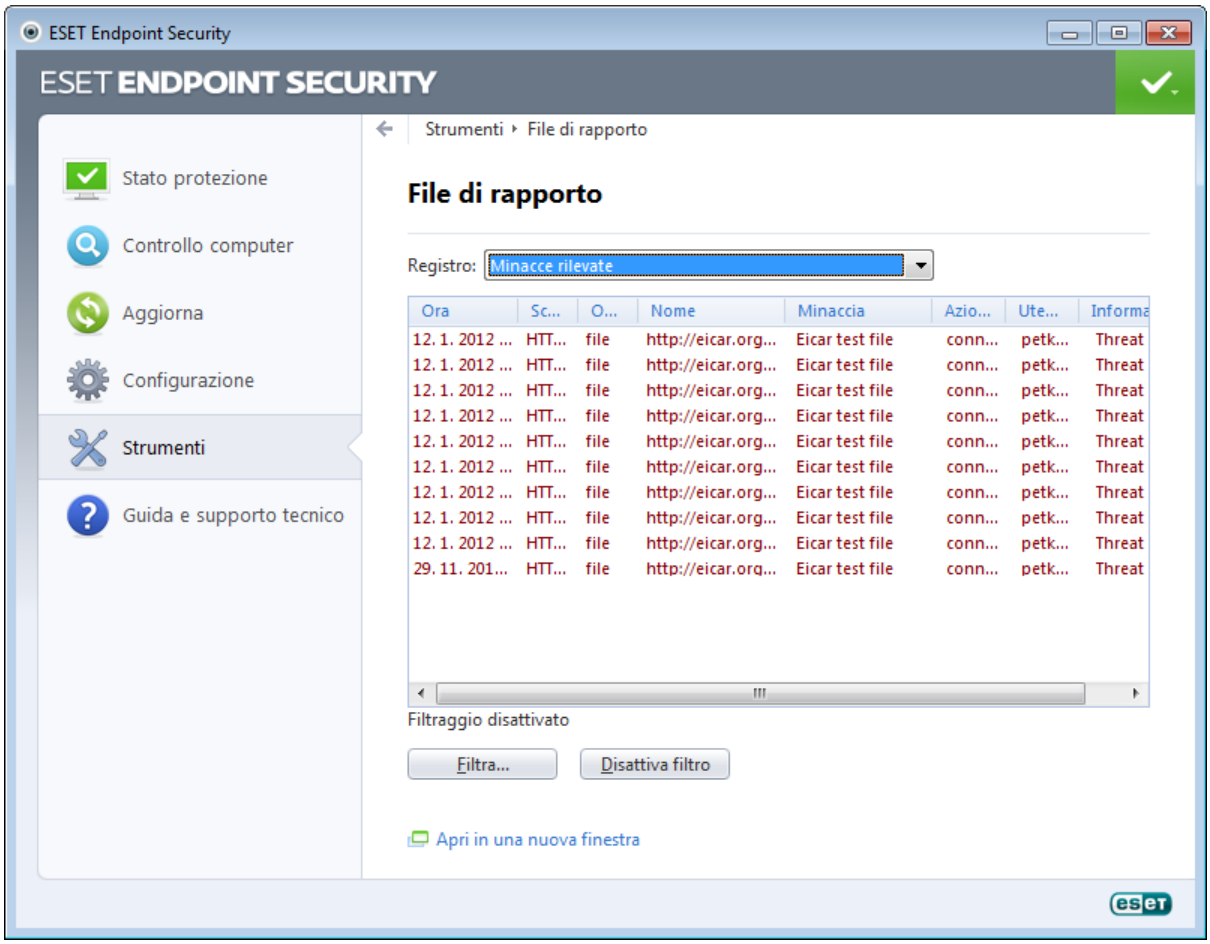
- File di rapporto
- Statistiche di protezione
- Attività di verifica
- Processi in esecuzione
- Pianificazione attività
- Quarantena
- Connessioni di rete
- ESET SysInspector

Invia file per analisi - Consente di inviare un file sospetto ai laboratori antivirus ESET per l'analisi. La finestra di dialogo visualizzata dopo aver selezionato questa opzione è descritta nella sezione Invio di file per l'analisi.

ESET SysRescue - Avvia la procedura di creazione guidata di ESET SysRescue.

4.6.1 File di rapporto

I file di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta uno strumento essenziale per l'analisi del sistema, il rilevamento delle minacce e la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto correnti. È possibile visualizzare i messaggi di testo e i rapporti direttamente dall'ambiente di ESET Endpoint Security, nonché dai registri di archivio.



È possibile accedere ai file di rapporto dalla finestra principale del programma facendo clic su **Strumenti** > **File di rapporto**. Selezionare il tipo di rapporto desiderato nel menu a discesa **Rapporto**. Sono disponibili i rapporti seguenti:

- **Minacce rilevate** - Nel rapporto delle minacce sono contenute informazioni dettagliate sulle infiltrazioni rilevate dai moduli ESET Endpoint Security. Le informazioni includono l'ora del rilevamento, il nome dell'infiltrazione, la posizione, l'azione eseguita e il nome dell'utente registrato nel momento in cui è stata rilevata l'infiltrazione. Fare doppio clic su una voce qualsiasi del rapporto per visualizzarne il contenuto dettagliato in una finestra separata.
- **Eventi** - Tutte le azioni importanti eseguite da ESET Endpoint Security vengono registrate nel rapporto eventi. Il rapporto eventi contiene informazioni sugli eventi e sugli errori che si sono verificati nel programma. È utile agli amministratori di sistema e agli utenti per risolvere i problemi. Spesso le informazioni visualizzate in questo rapporto consentono di trovare la soluzione a un problema che si verifica nel programma.
- **Controllo computer** - In questa finestra vengono visualizzati i risultati di tutti i controlli manuali o pianificati completati. Ogni riga corrisponde a un singolo controllo del computer. Fare doppio clic su una voce per visualizzare i dettagli del rispettivo controllo.
- **HIPS** - Contiene i record di regole specifiche che sono stati contrassegnati per la registrazione. Nel protocollo viene mostrata l'applicazione che ha invocato l'operazione, il risultato (ovvero se la regola era consentita o vietata) e il nome della regola creata.
- **Firewall personale** - Nel rapporto Firewall sono visualizzati tutti gli attacchi remoti rilevati dal Firewall personale. In questo rapporto è possibile trovare informazioni su tutti gli attacchi al computer in uso. Nella colonna Evento sono elencati gli attacchi rilevati. Nella colonna Origine vengono fornite ulteriori informazioni sull'autore dell'attacco. Nella colonna Protocollo viene indicato il protocollo di comunicazione usato per l'attacco. L'analisi del rapporto Firewall aiuta a rilevare le infiltrazioni al sistema in tempo utile per impedire l'accesso non autorizzato al sistema.

- **Protezione antispam** - Contiene record correlati ai messaggi e-mail contrassegnati come spam.
- **Controllo Web** - Mostra gli indirizzi URL bloccati o consentiti e le rispettive categorie. Nella colonna Azione eseguita sono indicate le regole di filtraggio applicate.
- **Controllo dispositivi** - Contiene record relativi ai supporti rimovibili o dispositivi collegati al computer. Nel file di rapporto saranno registrati solo i dispositivi con la rispettiva regola di controllo dispositivi. Se la regola non corrisponde a un dispositivo connesso, non verrà creata una voce di rapporto per un dispositivo connesso. Qui è possibile visualizzare dettagli quali il tipo di dispositivo, il numero di serie, il nome del fornitore e le dimensioni del supporto (se disponibili).

In ciascuna sezione, le informazioni visualizzate possono essere copiate direttamente negli Appunti (tasto di scelta rapida Ctrl + C), selezionando la voce desiderata e facendo clic su **Copia**. Per selezionare più voci, usare i tasti CTRL e MAIUSC.

Fare clic con il pulsante destro del mouse su un record specifico per visualizzare il menu contestuale. Nel menu contestuale sono disponibili le seguenti opzioni:

- **Filtra record dello stesso tipo** - Dopo aver attivato questo filtro, verranno visualizzati solo record dello stesso tipo (diagnostica, avvisi, ecc.).
- **Filtro.../Trova...** - Dopo aver selezionato questa opzione, viene visualizzata la finestra **Filtraggio rapporti** in cui è possibile definire i criteri di filtraggio.
- **Disattiva filtro** - Consente di annullare tutte le impostazioni del filtro (come descritto in precedenza).
- **Copia tutto** - Copia le informazioni su tutti i record nella finestra.
- **Elimina/Elimina tutto** - Elimina i record selezionati o tutti i record visualizzati. Per poter eseguire questa operazione è necessario disporre dei privilegi amministrativi.
- **Esporta** - Consente di esportare le informazioni sui record in formato XML.
- **Scorri registro** - Lasciare attivata questa opzione per scorrere i rapporti meno recenti e osservare i rapporti attivi nella finestra **File di rapporto**.

4.6.1.1 Manutenzione rapporto

La configurazione dei file di rapporto di ESET Endpoint Security è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Accedi a configurazione avanzata...** > **Strumenti** > **File di rapporto**. La sezione relativa ai file di rapporto viene utilizzata per definire le modalità di gestione dei rapporti. Il programma elimina automaticamente i rapporti meno recenti per liberare spazio sull'unità disco rigido. Per i file di rapporto è possibile specificare le opzioni seguenti:

Elimina automaticamente record più vecchi di (giorni): - Le voci del rapporto più vecchie del numero specificato di giorni verranno eliminate automaticamente.

Ottimizza automaticamente file di rapporto - Se questa opzione è selezionata, i file di rapporto vengono automaticamente deframmentati se la percentuale è superiore al valore specificato nel campo **Se il numero di record inutilizzati supera (%)**.

Fare clic su **Ottimizza ora** per avviare la deframmentazione dei file di rapporto. Durante questa procedura, tutte le voci vuote del rapporti vengono rimosse, con conseguente miglioramento delle prestazioni e della velocità del processo di elaborazione dei rapporti. Tale miglioramento può essere rilevato in particolare se i rapporti contengono un numero elevato di elementi.

Livello di dettaglio di registrazione minimo - Specifica il livello di dettaglio minimo degli eventi da registrare.

- **Diagnostica** - Registra tutte le informazioni necessarie per l'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativi** - Messaggi di record informativi che includono gli aggiornamenti riusciti e tutti i record indicati in precedenza.
- **Allarmi** - Consente di registrare errori critici e messaggi di allarme.
- **Errori** - Verranno registrati errori quali "Errore durante il download del file" ed errori critici.
- **Critici** - Registra solo gli errori critici (errore che avvia la protezione antivirus, il Firewall personalee così via).

Fare clic su **Attiva protocollo di testo** per archiviare i rapporti in un altro formato di file e all'esterno dei File di rapporto:

- **Tipo** - Scegliendo il formato del file di testo **Semplice**, i rapporti verranno archiviati in un file di testo e i dati verranno separati da tabulazioni. Lo stesso vale per il formato del file **CSV** separato da virgole. Scegliendo **Evento**, i rapporti verranno archiviati nel rapporto Eventi Windows (che è possibile visualizzare utilizzando il visualizzatore degli eventi nel Pannello di controllo) anziché nel file.
- **Directory di destinazione** - Punto di archiviazione dei file (valido solo per il formato testo semplice/CSV). Ciascuna sezione dei rapporti contiene il proprio file con un nome predefinito (ad esempio virlog.txt per la sezione**Minacce**

rilevate dei file di rapporto, se si utilizza il formato del file di testo semplice per l'archiviazione dei rapporti).

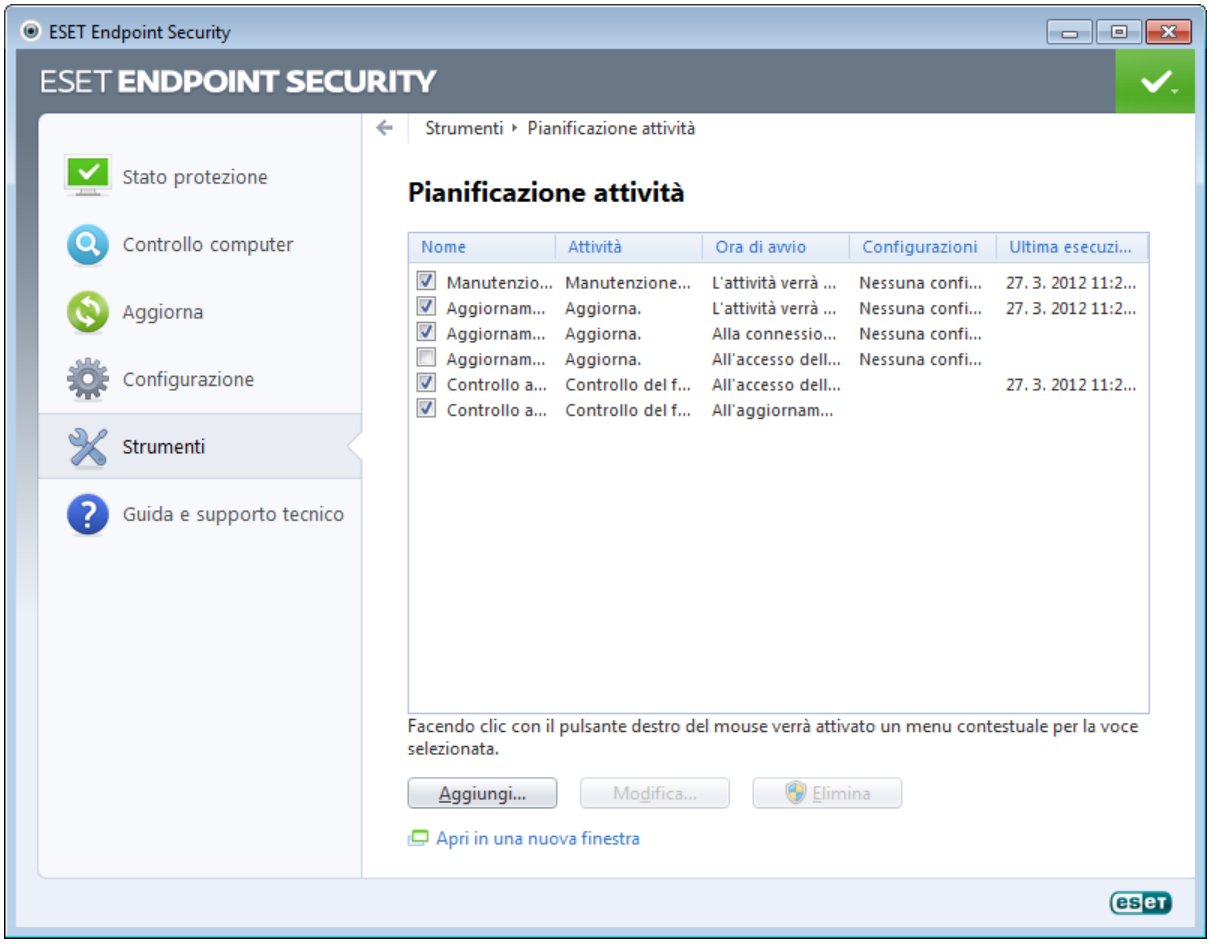
Il pulsante **Elimina rapporto** elimina tutti i rapporti archiviati attualmente selezionati nel menu a discesa **Tipo**.

4.6.2 Pianificazione attività

La Pianificazione attività consente di gestire e avviare attività pianificate con configurazione e proprietà predefinite.

È possibile accedere alla Pianificazione attività nella finestra principale del programma di ESET Endpoint Security facendo clic su **Strumenti** > **Pianificazione attività**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, ad esempio data, ora e profilo di controllo predefiniti utilizzati.

La Pianificazione attività consente di pianificare le attività seguenti: aggiornamento del database delle firme antivirali, attività di scansione, controllo dei file di avvio del sistema e manutenzione dei rapporti. È possibile aggiungere o modificare attività direttamente dalla finestra principale Pianificazione attività, facendo clic su **Aggiungi...** o **Elimina** nella parte inferiore della finestra. Fare clic con il pulsante destro del mouse in qualsiasi punto della finestra Pianificazione attività per eseguire le azioni seguenti: visualizzare informazioni dettagliate, eseguire immediatamente l'attività, aggiungere una nuova attività ed eliminare un'attività esistente. Utilizzare le caselle di controllo accanto a ciascuna voce per attivare o disattivare le attività.


ESET Endpoint Security
ESET ENDPOINT SECURITY
Strumenti ▸ Pianificazione attività
Stato protezione
Controllo computer
Aggiorna
Configurazione
Strumenti
Guida e supporto tecnico
Pianificazione attività
Nome
Attività
Ora di avvio
Configurazioni
Ultima esecuzi...
Manutenzio... Manutenzione... L'attività verrà ... Nessuna confi... 27. 3. 2012 11:2...
Aggiornam... Aggiorna. L'attività verrà ... Nessuna confi... 27. 3. 2012 11:2...
Aggiornam... Aggiorna. Alla connessio... Nessuna confi...
Aggiornam... Aggiorna. All'accesso dell... Nessuna confi...
Controllo a... Controllo del f... All'accesso dell... 27. 3. 2012 11:2...
Controllo a... Controllo del f... All'aggiornam...
Facendo clic con il pulsante destro del mouse verrà attivato un menu contestuale per la voce selezionata.
Aggiungi...
Modifica...
Elimina
Apri in una nuova finestra
eset

Per impostazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

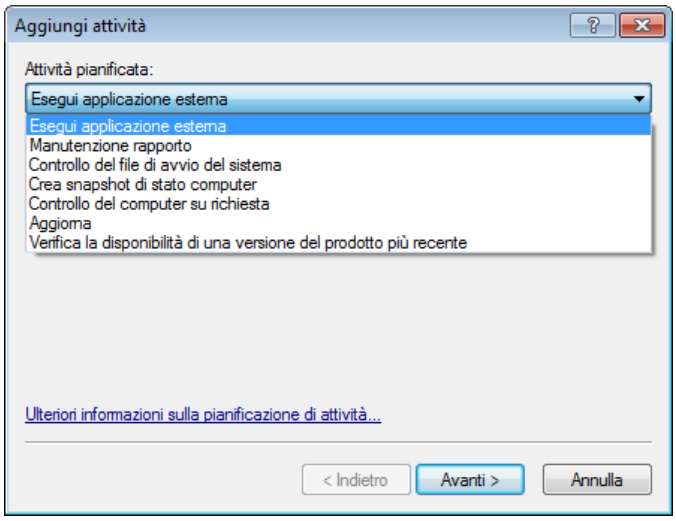
- **Manutenzione rapporto**
- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controllo automatico file di avvio** (dopo l'accesso utente)
- **Controllo automatico file di avvio** (dopo il completamento dell'aggiornamento del database delle firme antivirali)

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), fare clic con il pulsante destro del mouse sull'attività e selezionare **Modifica...** oppure selezionare l'attività che si desidera modificare e fare clic sul pulsante **Modifica...**.

Aggiunta di un nuova attività

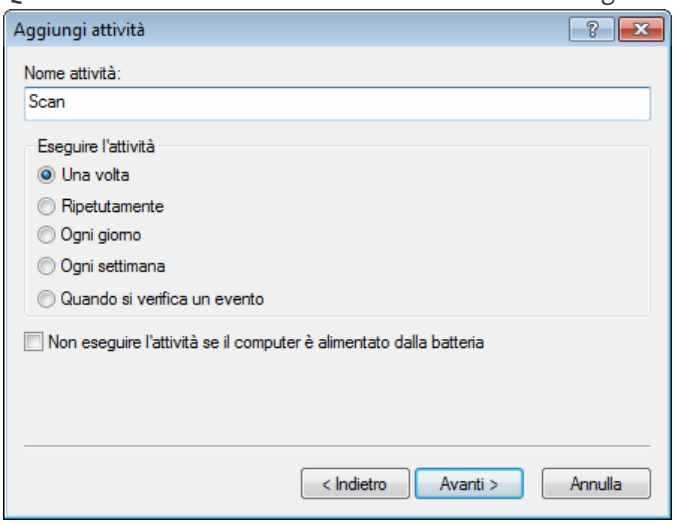
1. Fare clic su **Aggiungi...** nella parte inferiore della finestra.

2. Selezionare l'attività desiderata dal menu a discesa.



3. Immettere il nome dell'attività e selezionare l'intervallo di tempo desiderato:

- **Una volta** - L'attività verrà eseguita solo una volta, alla data e all'ora predefinite.
- **Ripetutamente** - L'attività verrà eseguita in base all'intervallo specificato (in ore).
- **Ogni giorno** - L'attività verrà eseguita ogni giorno all'ora specificata.
- **Ogni settimana** - L'attività verrà eseguita una o più volte alla settimana, nei giorni e nelle ore specificati.
- **Quando si verifica un evento** - L'attività verrà eseguita quando si verifica un evento specifico.



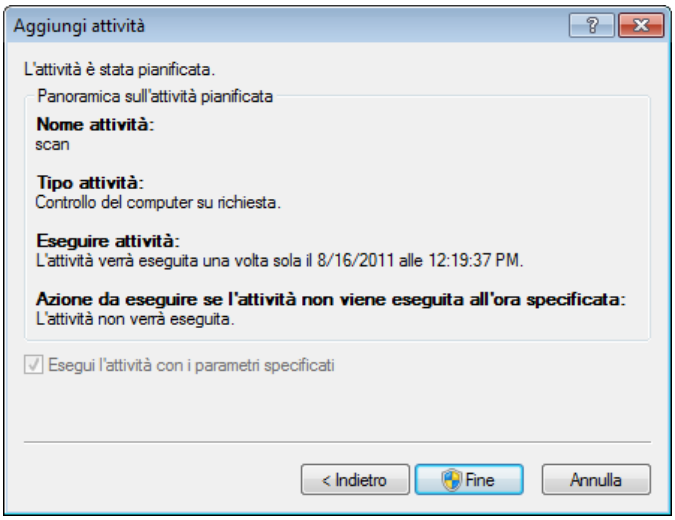
4. A seconda dell'intervallo di tempo selezionato nel passaggio precedente, verrà visualizzata una delle seguenti finestra di dialogo:

- **Una volta** - L'attività verrà eseguita alla data e all'ora predefinite.
- **Ripetutamente** - L'attività verrà eseguita in base all'intervallo di tempo specificato.
- **Ogni giorno** - L'attività verrà eseguita periodicamente ogni giorno all'ora specificata.
- **Ogni settimana** - L'attività verrà eseguita nel giorno e nell'ora selezionati.

5. Se l'attività non è stata eseguita all'ora predefinita, è possibile specificare il momento in cui dovrà essere nuovamente eseguita:

- Attendi l'ora pianificata successiva
- Esegui l'attività appena possibile
- Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera -- ore

6. Nell'ultimo passaggio, è possibile verificare l'attività da pianificare. Fare clic su **Fine** per confermare l'attività.



4.6.2.1 Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic sul pulsante **Aggiungi...** oppure fare clic con il tasto destro del mouse e selezionare **Aggiungi...** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna** - Consente di pianificare l'esecuzione di un'applicazione esterna.
- **Manutenzione rapporto** - File di rapporto contenenti elementi rimasti dai record eliminati. Questa attività ottimizza periodicamente i record nei file di rapporto allo scopo di garantire un funzionamento efficiente.
- **Controllo del file di avvio del sistema** - Consente di controllare i file la cui esecuzione è consentita all'avvio del sistema o all'accesso.
- **Crea snapshot di stato computer** - Consente di creare uno snapshot del computer ESET SysInspector (raccoglie informazioni dettagliate sui componenti del sistema, ad esempio driver e applicazioni, e valuta il livello di rischio di ciascun componente).
- **Controllo computer** - Consente di eseguire un controllo di file e di cartelle sul computer in uso.
- **Aggiorna** - Consente di pianificare un'attività di aggiornamento aggiornando il database delle firme antivirali e i moduli del programma.

Poiché **Aggiorna** rappresenta una delle attività pianificate utilizzata con maggiore frequenza, di seguito verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento.

Dal menu a discesa **Attività pianificata**, selezionare **Aggiorna**. Fare clic su **Avanti** e immettere il nome dell'attività nel campo **Nome attività**. Selezionare la frequenza dell'attività. Sono disponibili le seguenti opzioni: **Una volta**, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento**. Selezionare l'opzione **Non eseguire l'attività se il computer è alimentato dalla batteria** per ridurre al minimo l'utilizzo delle risorse del sistema quando il computer portatile è alimentato a batteria. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le tre opzioni riportate di seguito:

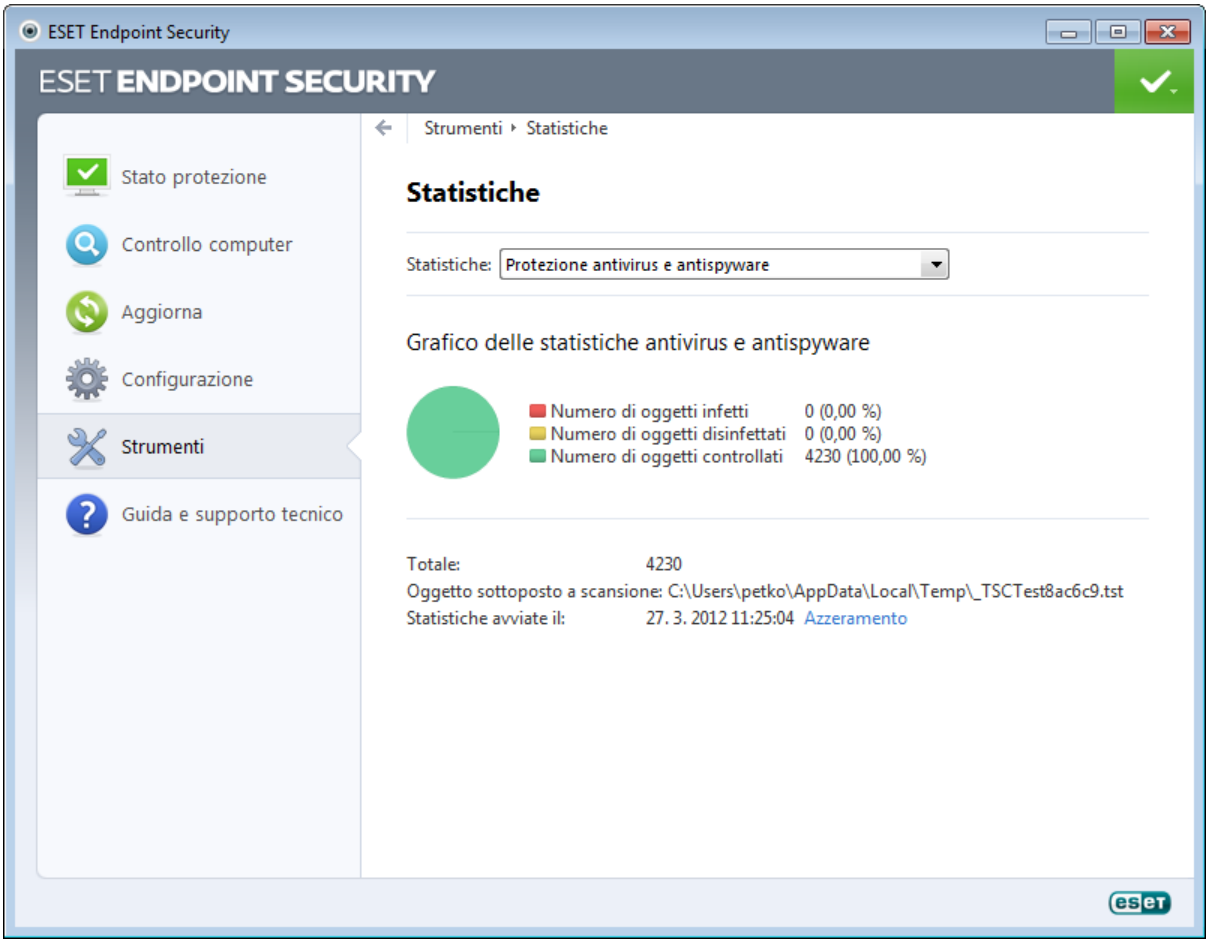
- **Attendi l'ora pianificata successiva**
- **Esegui attività appena possibile**
- **Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera l'intervallo specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento Intervallo attività)

Nel passaggio successivo, viene visualizzata una finestra contenente un riepilogo delle informazioni sull'attività pianificata corrente; l'opzione **Esegui attività con i parametri specificati** dovrebbe essere automaticamente abilitata. Fare clic sul pulsante **Fine**.

Verrà visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui è possibile indicare un profilo principale e uno alternativo, da utilizzare nel caso in cui l'attività non possa essere completata con il profilo principale. Confermare facendo clic su **OK** nella finestra **Aggiorna profili**. La nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

4.6.3 Statistiche di protezione

Per visualizzare un grafico dei dati statistici relativi ai moduli di protezione ESET Endpoint Security, fare clic su **Strumenti** > **Statistiche di protezione**. Selezionare il modulo di protezione desiderato dal menu a discesa **Statistiche** per visualizzare il grafico e la legenda corrispondenti. Se si passa il mouse su un elemento nella legenda, verranno visualizzati solo i dati di quell'elemento nel grafico.



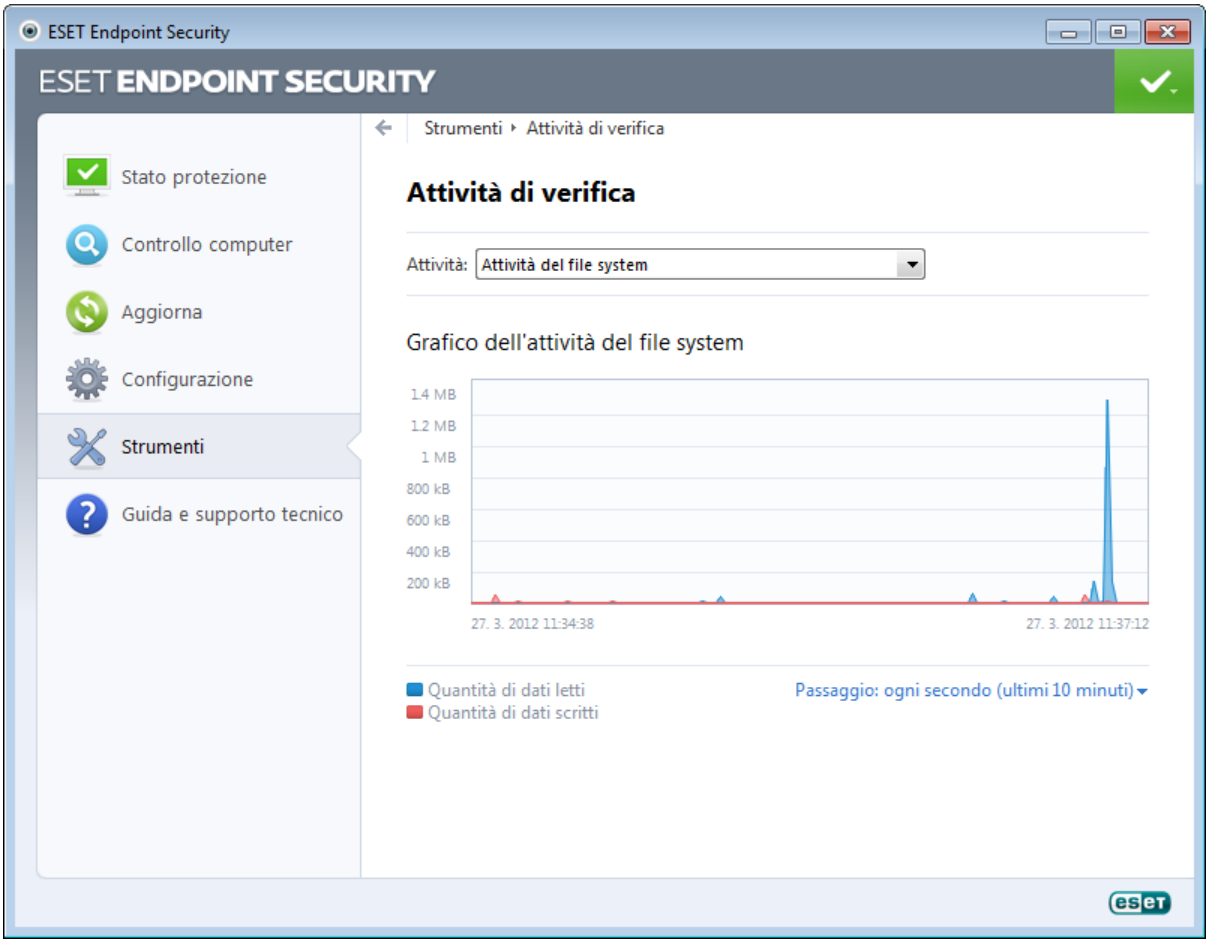
Sono disponibili i seguenti grafici statistici:

- **Protezione antivirus e antispyware** - Consente di visualizzare il numero di oggetti infetti e puliti.
- **Protezione file system** - Consente di visualizzare solo gli oggetti che sono stati scritti o letti sul file system.
- **Protezione client e-mail** - Consente di visualizzare solo gli oggetti inviati o ricevuti dai client e-mail.
- **Protezione accesso Web** - Consente di visualizzare solo gli oggetti scaricati dai browser Internet.
- **Protezione antispam client e-mail** - Consente di visualizzare la cronologia delle statistiche antispam dall'ultimo avvio.

Sotto il grafico delle statistiche è visualizzato il numero degli oggetti totali sottoposti a controllo, l'ultimo oggetto sottoposto a controllo e la data e l'ora delle statistiche. Fare clic su **Azzeramento** per cancellare tutte le informazioni statistiche.

4.6.4 Attività di verifica

Per visualizzare l'**Attività di file system** corrente in un grafico, fare clic su **Strumenti** > **Attività di verifica**. Sotto al grafico è visualizzata una linea cronologica che registra in tempo reale le attività di file system in base all'intervallo di tempo selezionato. Per modificare l'intervallo di tempo, fare clic sull'opzione **Passaggo: ogni...** in basso a destra della finestra.



Sono disponibili le seguenti opzioni:

- **Passaggio: ogni secondo (ultimi 10 minuti)** - Il grafico si aggiorna ogni secondo e l'intervallo di tempo copre gli ultimi 10 minuti
- **Passaggio: ogni minuto (ultime 24 ore)** - Il grafico si aggiorna ogni minuto e l'intervallo di tempo copre le ultime 24 ore
- **Passaggio: ogni ora (ultimo mese)** - Il grafico si aggiorna ogni ora e l'intervallo di tempo copre l'ultimo mese
- **Passaggio: ogni ora (mese selezionato)** - Il grafico si aggiorna ogni ora e l'intervallo di tempo copre gli ultimi X mesi selezionati

L'asse verticale del **Grafico dell'attività del file system** rappresenta i dati letti (blu) e scritti (rosso). Entrambi i valori sono espressi in KB (kilobyte)/MB/GB. Facendo scorrere il mouse sui dati letti o scritti nella didascalia sottostante il grafico, è possibile visualizzare unicamente i dati relativi a quella specifica attività.

Nel menu a discesa **Attività** è inoltre possibile visualizzare l'**Attività di rete**. La visualizzazione del grafico e le opzioni per l'**Attività di file system** e l'**Attività di rete** sono uguali tranne per il fatto che in quest'ultima i dati ricevuti sono visualizzati in blu e quelli inviati in rosso.

4.6.5 ESET SysInspector

ESET SysInspector è un'applicazione che esamina a fondo il computer, raccoglie informazioni dettagliate sui componenti del sistema, quali i driver e le applicazioni installati, le connessioni di rete o le voci di registro importanti e valuta il livello di rischio di ciascun componente. Tali informazioni possono risultare utili per determinare la causa di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

Nella finestra di dialogo SysInspector sono visualizzate le seguenti informazioni sui rapporti creati:

- **Ora** - Ora di creazione del rapporto.
- **Commento** - Breve commento.
- **Utente** - Nome dell'utente che ha creato il rapporto.
- **Stato** - Stato di creazione del rapporto.

Sono disponibili le azioni seguenti:

- **Confronta** - Consente di mettere a confronto due rapporti esistenti.
- **Crea...** - Consente di creare un nuovo rapporto. Attendere il completamento del rapporto di ESET SysInspector (**Stato**: Creato).
- **Elimina** - Rimuove dall'elenco i rapporti selezionati.

Fare clic con il pulsante destro del mouse su uno o più rapporti selezionati per visualizzare le opzioni seguenti del menu contestuale:

- **Mostra** - Visualizza il rapporto selezionato in ESET SysInspector (funzione uguale all'esecuzione di un doppio clic su un rapporto).
- **Elimina tutto** - Consente di eliminare tutti i rapporti.
- **Esporta...** - Esporta il rapporto su un file XML o su un file XML compresso.

4.6.6 ESET Live Grid

ESET Live Grid(la nuova generazione di ESET ThreatSense.Net) è un sistema avanzato di allarme contro le minacce emergenti basato sulla reputazione. Utilizzando il flusso in tempo reale delle informazioni correlate alla minacce proveniente dal cloud, i laboratori antivirus ESET mantengono aggiornate le difese per assicurare un livello di protezione costante. L'utente può controllare la reputazione dei processi in esecuzione e dei file direttamente dall'interfaccia del programma o dal menu contestuale. Ulteriori informazioni sono inoltre disponibili su ESET Live Grid. Sono disponibili due opzioni:

1. È possibile decidere di non abilitare ESET Live Grid. Non verranno perse funzionalità del software, che continuerà ad offrire la migliore protezione in assoluto.
2. È possibile configurare ESET Live Grid per l'invio di informazioni anonime sulle nuove minacce e laddove sia presente il nuovo codice dannoso. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce sarà d'aiuto ad ESET per aggiornare le proprie capacità di rilevamento.

ESET Live Grid raccoglierà informazioni sul computer degli utenti in relazione alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso al file, il nome del file, informazioni su data e ora, il processo in base al quale la minaccia è apparsa sul computer e informazioni sul sistema operativo del computer.

Per impostazione predefinita, ESET Endpoint Security è configurato per l'invio dei file sospetti per l'analisi dettagliata ai laboratori antivirus ESET. Sono sempre esclusi file con determinate estensioni, ad esempio DOC o XLS. È inoltre possibile aggiungere altre estensioni qualora sussistano specifici file che l'utente o la società dell'utente non desidera inviare.

Nel menu di configurazione di ESET Live Grid sono disponibili diverse opzioni per attivare/disattivare ESET Live Grid da utilizzare per l'invio dei file sospetti e delle informazioni statistiche anonime ai laboratori ESET. È accessibile dalla struttura di Configurazione avanzata selezionando **Strumenti** > **ESET Live Grid**.

Partecipa a ESET Live Grid - Consente di attivare/disattivare ESET Live Grid da utilizzare per l'invio dei file sospetti e delle informazioni statistiche anonime ai laboratori ESET.

Non inviare statistiche - Selezionare questa opzione se non si desidera inviare informazioni anonime sul computer mediante ESET Live Grid. Queste informazioni sono correlate alle minacce più recenti rilevate e possono comprendere il nome dell'infiltrazione, la data e l'ora del rilevamento, la versione di ESET Endpoint Security, la versione del sistema operativo in uso e le impostazioni di ubicazione. Di norma, le statistiche vengono inviate al server di ESET una o due volte al giorno.

Non inviare file - I file sospetti che somigliano a infiltrazioni per il loro contenuto o comportamento non vengono inviati a ESET per essere analizzati con la tecnologia ESET Live Grid.

Configurazione avanzata... - Apre una finestra contenente ulteriori impostazioni per ESET Live Grid.

Se ESET Live Grid è già stato utilizzato in precedenza ed è stato disattivato, potrebbero essere ancora presenti pacchetti di dati da inviare. Anche dopo la disattivazione, tali pacchetti verranno inviati a ESET all'occasione successiva. Successivamente, non verrà più creato alcun pacchetto.

4.6.6.1 File sospetti

La scheda **File** nella Configurazione avanzata di ESET Live Grid consente di configurare il modo in cui le minacce vengono inviate al laboratorio ESET preposto allo studio delle minacce per sottoporle ad analisi.

Se si rileva un file sospetto, è possibile inviarlo per l'analisi ai ThreatLabs. Se viene individuata un'applicazione dannosa, essa verrà aggiunta al successivo aggiornamento delle firme antivirali.

Filtro di esclusione - Il Filtro di esclusione consente di escludere dall'invio determinati file/cartelle. I file elencati non verranno mai inviati ai laboratori ESET per l'analisi, anche se contengono codice sospetto. È ad esempio utile escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (con estensione DOC e così via). È possibile aggiungerli alla lista degli elementi esclusi dalla scansione.

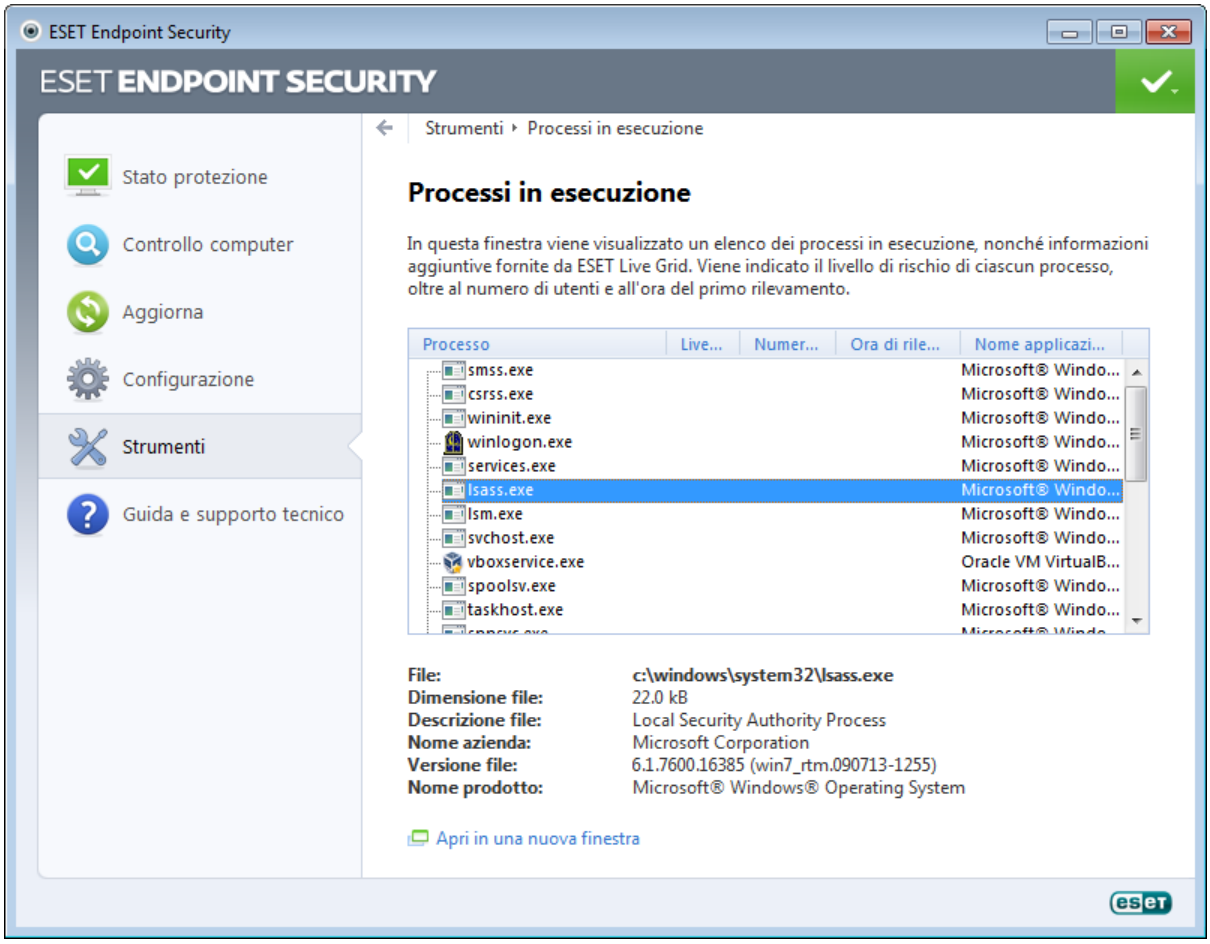
Contatto e-mail (facoltativo) - Il contatto e-mail può essere inviato insieme ai file sospetti e potrebbe essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

In questa sezione è anche possibile scegliere se inviare i file e le informazioni statistiche tramite ESET Remote Administrator o direttamente a ESET. Se si desidera essere certi che i file sospetti e le informazioni statistiche siano consegnati a ESET, selezionare l'opzione **Tramite Remote Administrator o direttamente a ESET**. In questo caso, i file e le statistiche vengono inviati mediante tutti i mezzi disponibili. L'invio dei file sospetti tramite Remote Administrator consente di inviare i file e le statistiche al server di amministrazione remota, garantendo così il successivo invio ai laboratori antivirus ESET. Se si seleziona l'opzione **Direttamente a ESET**, tutti i file sospetti e le informazioni statistiche vengono inviati ai laboratori antivirus ESET direttamente dal programma.

Selezionare l'opzione **Attiva rapporto** per creare un rapporto eventi sul quale sono registrati gli invii dei file e delle informazioni statistiche. Consente la registrazione sul Rapporto eventi durante l'invio di file o statistiche.

4.6.7 Processi in esecuzione

I processi in esecuzione consentono di visualizzare i programmi o processi in esecuzione sul computer e inviare informazioni tempestive e costanti a ESET sulle nuove infiltrazioni. ESET Endpoint Security fornisce informazioni dettagliate sui processi in esecuzione allo scopo di proteggere gli utenti che utilizzano la tecnologia ESET Live Grid.



Processo - Nome immagine del programma o del processo attualmente in esecuzione sul computer. Per visualizzare tutti i processi in esecuzione sul computer è inoltre possibile utilizzare Windows Task Manager. Per aprire Task Manager, fare clic con il pulsante destro del mouse su un'area vuota sulla barra delle attività, quindi scegliere Task Manager oppure premere Ctrl+Maiusc+Esc sulla tastiera.

Livello rischio - Nella maggior parte dei casi, ESET Endpoint Security e la tecnologia ESET Live Grid assegnano livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ogni oggetto e quindi ne valutano le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso).

NOTA: le applicazioni note contrassegnate come Non a rischio (verde) sono definite pulite (inserite nella whitelist) e saranno escluse dal controllo in modo da aumentare la velocità di esecuzione del controllo del computer su richiesta o della protezione file system in tempo reale sul computer.

Numero di utenti - Numero di utenti che utilizzano una determinata applicazione. Queste informazioni sono raccolte mediante la tecnologia ESET Live Grid.

Ora di rilevamento - Periodo di tempo da quando l'applicazione è stata rilevata dalla tecnologia ESET Live Grid.

NOTA: se un'applicazione è contrassegnata con un livello di rischio Sconosciuto (arancione), non si tratta necessariamente di software dannoso. In genere si tratta di una nuova applicazione. In caso di dubbi sul file, selezionare l'opzione invia file per analisi ai laboratori antivirus ESET. Se il file si rivela essere un'applicazione dannosa, il suo rilevamento verrà aggiunto in uno degli aggiornamenti successivi.

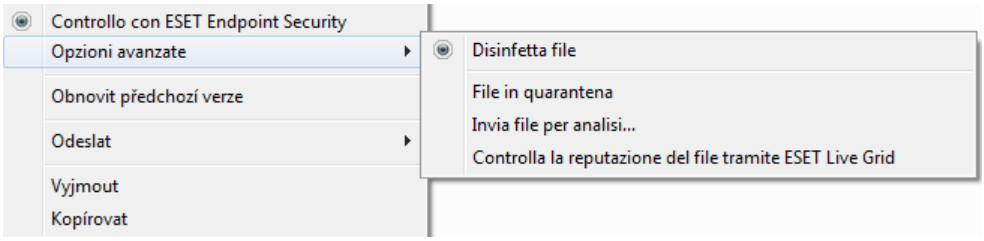
Nome applicazione - Nome specifico di un programma o processo.

Apri una nuova finestra - Le informazioni sui processi in esecuzione verranno visualizzate in una nuova finestra.

Fare clic sulla parte inferiore di una determinata applicazione per visualizzare le seguenti informazioni nella parte inferiore della finestra:

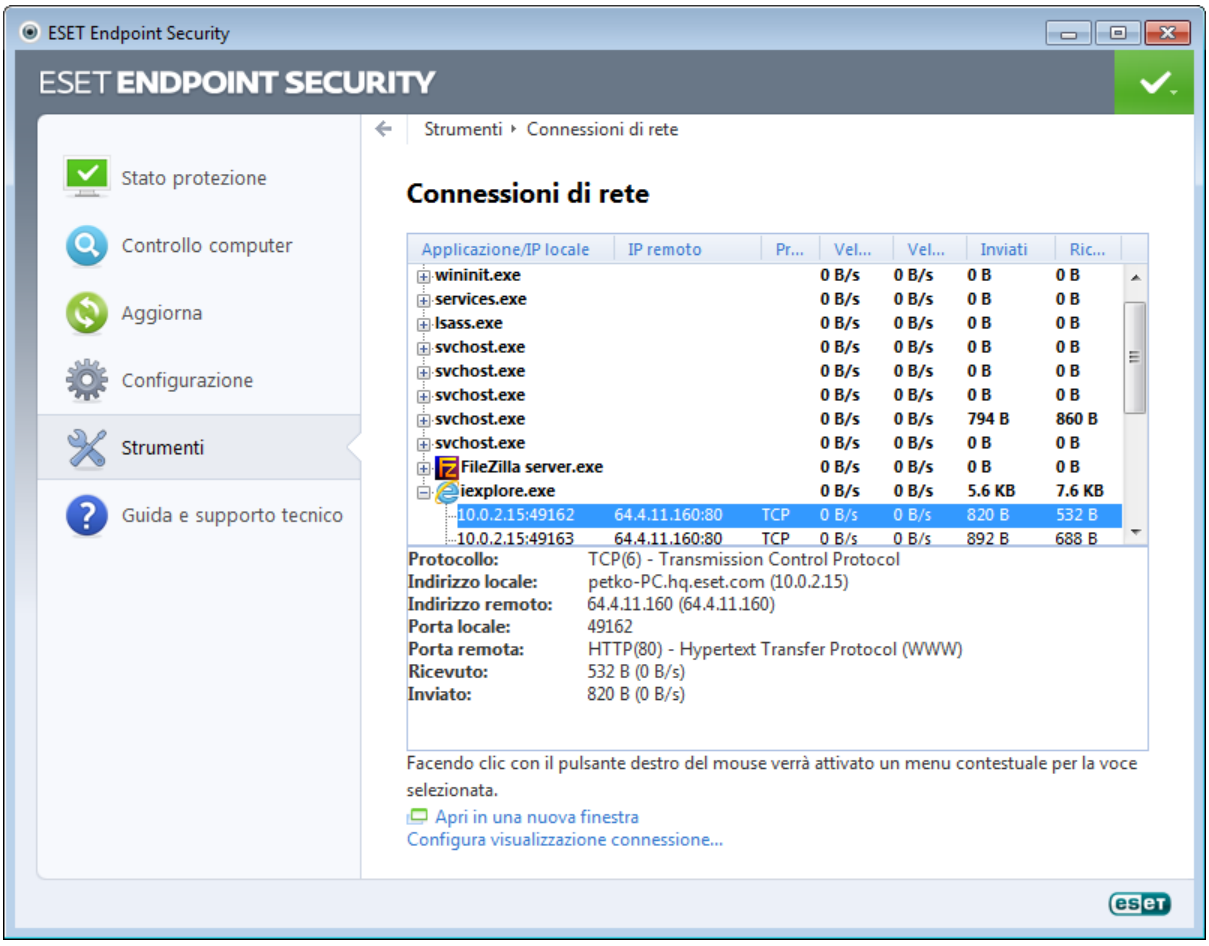
- **File** - Posizione di un'applicazione sul computer.
- **Dimensioni file** - Dimensione del file in kB (kilobyte) o MB (megabyte).
- **Descrizione file** - Caratteristiche del file basate sulla relativa descrizione del sistema operativo.
- **Nome società** - Nome del fornitore o del processo applicativo.
- **Versione file** - Informazioni estrapolate dall'autore dell'applicazione.
- **Nome prodotto** - Nome dell'applicazione e/o nome commerciale.

NOTA: la reputazione può essere controllata anche sui file che non agiscono come programmi/processi in esecuzione: contrassegnare i file che si desidera controllare, fare clic con il pulsante destro del mouse su di essi e nel menu contestuale selezionare **Opzioni avanzate** > **Controlla la reputazione del file tramite ESET Live Grid**.



4.6.8 Connessioni di rete

Nella sezione Connessioni di rete è possibile visualizzare l'elenco delle connessioni attive e in attesa. In questo modo è possibile controllare tutte le applicazioni che stabiliscono connessioni in uscita.



Sulla prima riga viene mostrato il nome dell'applicazione e la relativa velocità di trasferimento dati. Per visualizzare l'elenco delle connessioni effettuate dall'applicazione (e per maggiori informazioni), fare clic su **+**.

Applicazione/IP locale - Nome dell'applicazione, indirizzi IP e porte di comunicazione locali.

IP remoto - Indirizzo IP e numero di porta di un determinato computer remoto.

Protocollo - Protocollo di trasferimento utilizzato.

Velocità massima/Velocità minima - La velocità corrente dei dati in uscita e in entrata.

Inviati/Ricevuti - Quantità di dati scambiati durante la connessione.

Apri una nuova finestra - Visualizza le informazioni in una finestra separata.

L'opzione **Configura visualizzazione connessione...** nella schermata Connessioni di rete consente di accedere alla sezione della struttura della configurazione avanzata per modificare le opzioni di visualizzazione della connessione:

Risolvi nomi host - Se possibile, tutti gli indirizzi di rete sono visualizzati in formato DNS e non in formato indirizzo IP numerico.

Visualizza solo connessioni su protocollo TCP - Nell'elenco vengono visualizzate solo le connessioni che appartengono al protocollo TCP.

Visualizza connessioni con porte aperte sulle quali il computer è in ascolto - Selezionare questa opzione per visualizzare solo le connessioni in cui non è attualmente stabilita alcuna comunicazione ma per cui il sistema ha aperto una porta ed è in attesa di una connessione.

Visualizza anche le connessioni all'interno del computer - Selezionare questa opzione per visualizzare solo le connessioni in cui il lato remoto è costituito da un sistema locale, ovvero le connessioni dell'host locale.

Fare clic con il pulsante destro del mouse per visualizzare le opzioni aggiuntive che includono:

Nega comunicazione per la connessione - Interrompe la comunicazione stabilita. Questa opzione è disponibile solo dopo aver selezionato una connessione attiva.

Mostra dettagli - Scegliere questa opzione per visualizzare informazioni dettagliate sulla connessione selezionata.

Aggiorna velocità - Scegliere la frequenza di aggiornamento delle connessioni attive.

Aggiorna ora - Aggiorna la finestra Connessioni di rete.

Le opzioni seguenti sono disponibili solo dopo aver selezionato un'applicazione o un processo e non una connessione attiva:

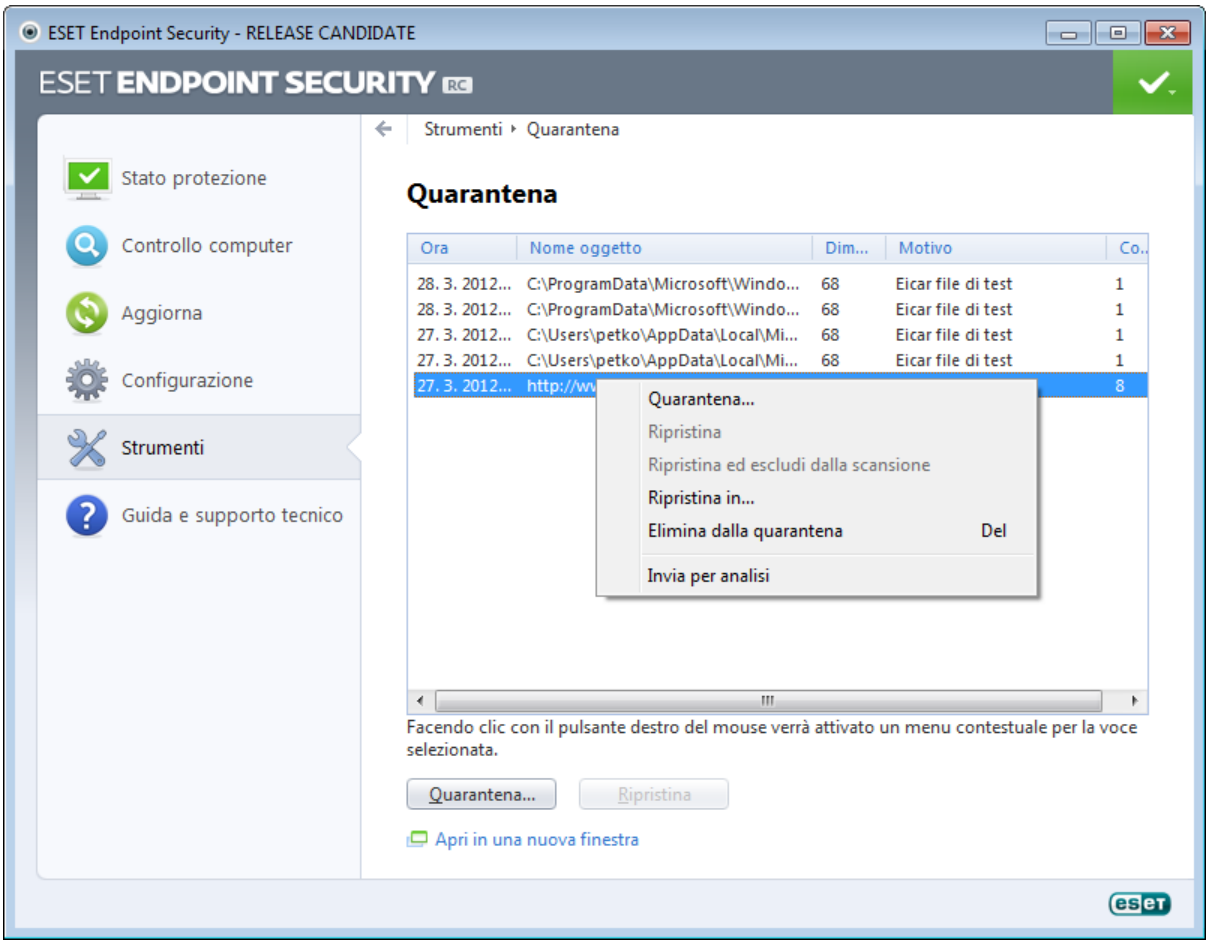
Nega temporaneamente comunicazione per il processo - Rifiuta le connessioni correnti dell'applicazione specificata. Se viene stabilita una nuova connessione, il firewall utilizza una regola predefinita. Per una descrizione delle impostazioni, consultare la sezione Regole e aree.

Consenti temporaneamente comunicazione per il processo - Consente le connessioni correnti dell'applicazione specificata. Se viene stabilita una nuova connessione, il firewall utilizza una regola predefinita. Per una descrizione delle impostazioni, consultare la sezione Regole e aree.

4.6.9 Quarantena

La funzione principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET Endpoint Security.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati ai laboratori antivirus ESET per l'analisi.



I file salvati nella cartella di quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio, aggiunto dall'utente) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni).

Mettere file in quarantena

ESET Endpoint Security mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto ad annullare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando **Quarantena...**. In tal caso, il file originale non verrà rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare l'opzione **Quarantena...**.

Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Utilizzare a tale scopo la funzione **Ripristina**, disponibile nel menu contestuale visualizzato facendo clic con il pulsante destro del mouse sul file desiderato nella finestra Quarantena. Se un file è contrassegnato come applicazione potenzialmente indesiderata, l'opzione **Ripristina ed escludi dalla scansione** è attivata. Per ulteriori informazioni su questo tipo di applicazione, consultare la relativa voce del glossario. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

NOTA: se il programma ha messo in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

Invio di un file dalla cartella Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena, o se un file è stato valutato erroneamente come infetto (ad esempio da un'analisi euristica del codice) e quindi messo in quarantena, inviare il file ai laboratori antivirus ESET. Per inviare un file dalla cartella di quarantena, fare clic con il pulsante destro del mouse sul file e selezionare **Invia per analisi** dal menu contestuale.

4.6.10 Invio di file per l'analisi

La finestra di dialogo per l'invio dei file consente di inviare un file a ESET ai fini dell'analisi ed è disponibile tramite **Strumenti** > **Invia file per analisi**. Se sul computer in uso è stato trovato un file con un comportamento sospetto, è possibile inviarlo ai laboratori ESET affinché sia analizzato. Se il file si rivela essere un'applicazione dannosa, il suo rilevamento verrà aggiunto in uno degli aggiornamenti successivi.

In alternativa, è possibile inviare il file tramite e-mail. Se si preferisce questa opzione, comprimere il file o i file con WinRAR/ZIP, proteggere l'archivio con la password "infected" e inviarlo a samples@eset.com. Ricordare di inserire una descrizione nel campo dell'oggetto e di fornire il maggior numero possibile di informazioni sul file, ad esempio l'indirizzo del sito Web dal quale è stato scaricato.

NOTA: Prima di inviare un file a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:
- il file non viene rilevato,
- il file viene erroneamente rilevato come una minaccia.

Non verrà inviata alcuna risposta a meno che non siano richieste ulteriori informazioni ai fini dell'analisi.

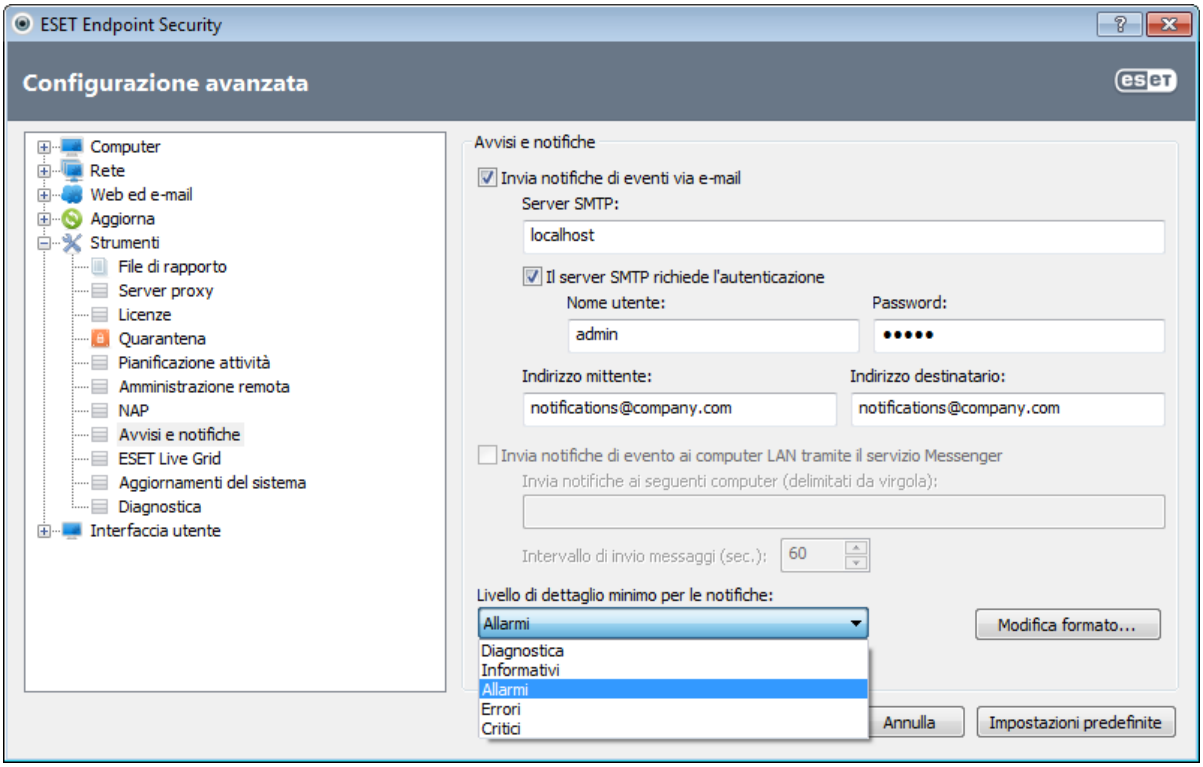
Selezionare la descrizione dal menu a discesa **Motivo per l'invio del file** che si avvicina maggiormente alla propria motivazione:
- **File sospetto**,
- **Falso positivo** (file che è stato rilevato come un'infezione ma che non è infetto),
- e **Altro**

File - Il percorso del file che si intende inviare.

E-mail contatto - Una e-mail di contatto viene inviata a ESET insieme ai file sospetti e può essere utilizzata per contattare il mittente qualora fossero necessarie ulteriori informazioni ai fini dell'analisi. L'immissione dell'indirizzo e-mail di contatto è facoltativa. ESET non invierà alcuna risposta a meno che non siano richieste ulteriori informazioni. Ogni giorno i server ESET ricevono decine di migliaia di file e non è pertanto possibile rispondere a tutti.

4.6.11 Avvisi e notifiche

ESET Endpoint Security supporta l'invio di e-mail nel caso in cui si verifichi un evento con il livello di dettaglio selezionato. Selezionare la casella di controllo **Invia notifiche di eventi via e-mail** per attivare questa funzione e le notifiche e-mail.



Server SMTP - Il server SMTP utilizzato per l'invio delle notifiche.

Nota: ESET Endpoint Security non supporta i server SMTP con crittografia SSL/TLS.

Il server SMTP richiede l'autenticazione - Se il server SMTP richiede l'autenticazione, questi campi devono essere compilati con nome utente e password validi per l'accesso al server SMTP.

Indirizzo mittente - Questo campo specifica l'indirizzo del mittente che verrà visualizzato nell'intestazione delle e-mail di notifica.

Indirizzo destinatario - Questo campo specifica l'indirizzo del destinatario che verrà visualizzato nell'intestazione delle e-mail di notifica.

Invia notifiche di evento ai computer LAN tramite il servizio Messenger - Selezionare questa casella di controllo per inviare messaggi ai computer LAN tramite il servizio Messenger di Windows®.

Invia notifiche ai seguenti computer (delimitati da virgola) - Immettere i nomi dei computer che riceveranno le notifiche tramite il servizio Messenger di Windows®.

Intervallo di invio messaggi (sec.) - Per modificare la lunghezza dell'intervallo tra le notifiche inviate tramite LAN, immettere l'intervallo di tempo desiderato in secondi.

Livello di dettaglio minimo per le notifiche - Specifica il livello di dettaglio minimo delle notifiche da inviare.

Modifica formato... - Le comunicazioni tra il programma e un utente remoto o un amministratore di sistema avvengono tramite e-mail o messaggi LAN (utilizzando il servizio Messenger di Windows®. Il formato predefinito dei messaggi e delle notifiche di avviso è adatto alla maggior parte delle situazioni. Tuttavia, qualora fosse necessario modificare il formato del messaggio, fare clic su Modifica formato....

4.6.11.1 Formato dei messaggi

In questa sezione è possibile configurare il formato dei messaggi di evento che vengono visualizzati sui computer remoti.

Gli avvisi di minaccia e i messaggi di notifica dispongono di un formato predefinito. Si consiglia di non modificare questo formato. Tuttavia, in alcuni casi (ad esempio, se si dispone di un sistema di elaborazione della posta automatizzato) potrebbe essere necessario modificare il formato dei messaggi.

Nel messaggio, le parole chiave (stringhe separate dai segni %) vengono sostituite dalle informazioni effettive specificate. Sono disponibili le parole chiave seguenti:

- **%TimeStamp%** - Data e ora dell'evento.
- **%Scanner%** - Modulo interessato.
- **%ComputerName%** - Nome del computer in cui si è verificato l'avviso.
- **%ProgramName%** - Programma che ha generato l'avviso.
- **%InfectedObject%** - Nome del file o del messaggio infetto.
- **%VirusName%** - Identificazione dell'infezione.
- **%ErrorDescription%** - Descrizione di un evento non virus.

Le parole chiave **%InfectedObject%** e **%VirusName%** vengono utilizzate solo nei messaggi di allarme per minacce, mentre **%ErrorDescription%** viene utilizzata solo nei messaggi di evento.

Utilizza caratteri alfabetici locali - Converte un messaggio e-mail nella codifica dei caratteri ANSI in base alle impostazioni della lingua di Windows (ad esempio windows-1250). Se si lascia deselezionata questa opzione, il messaggio verrà convertito e codificato in ACSII a 7-bit (ad esempio, "á" verrà modificata in "a" e un simbolo sconosciuto verrà modificato in "?").

Utilizza codifica caratteri locali - L'origine del messaggio e-mail verrà codificata in formato QP (Quoted-printable) che utilizza i caratteri ASCII ed è in grado di trasmettere correttamente speciali caratteri nazionali tramite e-mail nel formato a 8-bit (áéíóú).

4.6.12 Aggiornamenti del sistema

La funzione di aggiornamento di Windows è un componente importante per la protezione del computer da software dannosi. Per questo motivo, è fondamentale installare gli aggiornamenti di Microsoft Windows non appena vengono resi disponibili. ESET Endpoint Security fornisce avvisi riguardo gli aggiornamenti mancanti in base al livello indicato dall'utente. Sono disponibili i livelli seguenti:

- **Nessun aggiornamento** - Per il download non viene offerto nessun aggiornamento del sistema.
- **Aggiornamenti facoltativi** - Per il download vengono offerti aggiornamenti con priorità bassa e di livello superiore.
- **Aggiornamenti consigliati** - Per il download vengono offerti aggiornamenti contrassegnati come comuni o di livello superiore.
- **Aggiornamenti importanti** - Per il download vengono offerti aggiornamenti contrassegnati come importanti o di livello superiore.
- **Aggiornamenti critici** - Per il download vengono offerti unicamente gli aggiornamenti critici.

Fare clic su **OK** per salvare le modifiche. Dopo la verifica dello stato mediante il server di aggiornamento, viene visualizzata la finestra Aggiornamenti del sistema. Le informazioni sull'aggiornamento del sistema non saranno pertanto disponibili immediatamente dopo il salvataggio delle modifiche.

4.6.13 Diagnostica

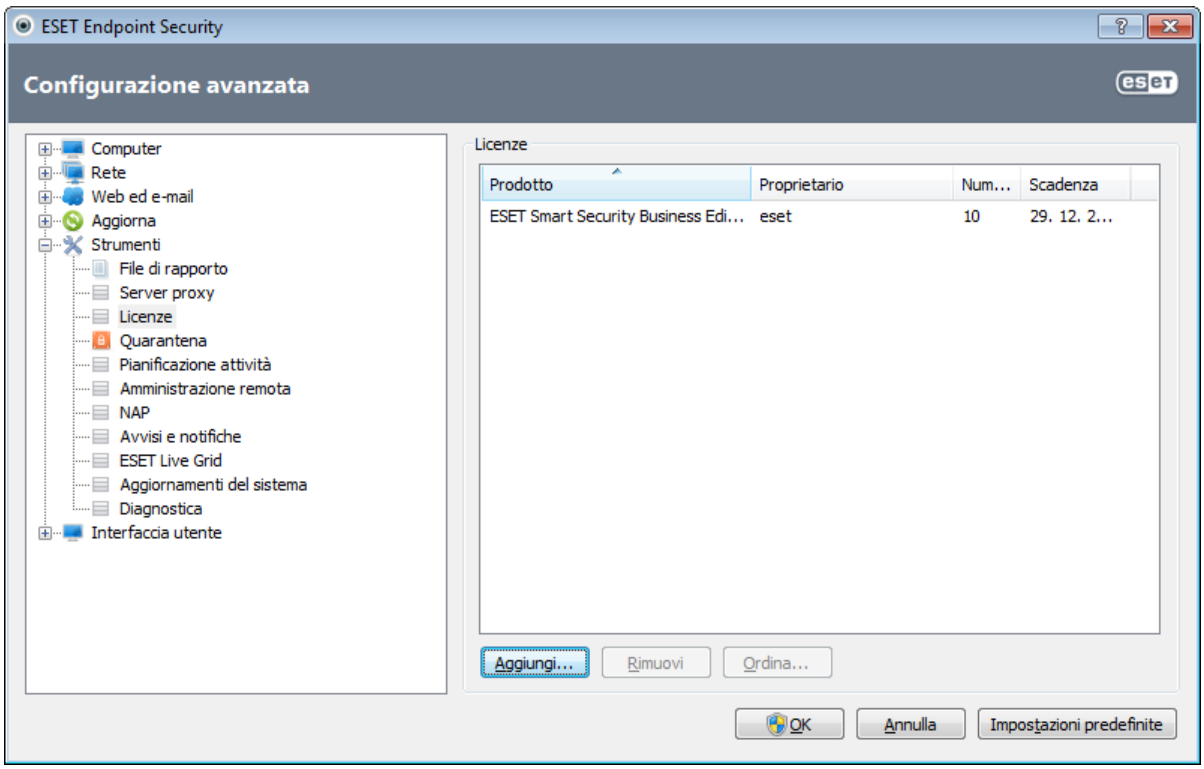
La diagnostica fornisce dump sulle interruzioni delle applicazioni correlate ai processi ESET, ad esempio ekrn. In caso di interruzione di un'applicazione, verrà generato un dump, che può aiutare gli sviluppatori a eseguire il debug e correggere vari problemi di ESET Endpoint Security. Sono disponibili due tipi di dump:

- **Dump memoria completo** - Registra tutti i contenuti della memoria di sistema quando l'applicazione viene interrotta inaspettatamente. Un dump memoria completo può contenete dati estrapolati dai processi in esecuzione quando è stato raccolto il dump di memoria.
- **Minidump** - Registra il minor numero possibile di informazioni utili che possono aiutare a identificare il motivo alla base dell'arresto inaspettato dell'applicazione. Questo tipo di file dump risulta utile in caso di limitazioni di spazio. A causa delle informazioni limitate incluse, gli errori che non sono stati causati direttamente dalla minaccia in esecuzione quando si è verificato il problema potrebbero tuttavia non essere rilevati a seguito di un'analisi del file in questione.
- Selezionare **Non generare dump di memoria** (impostazione predefinita) per disattivare questa funzione.

Directory di destinazione - Directory nella quale verrà generato il dump durante l'arresto imprevisto. Fare clic su **Apri cartella...** per aprire questa directory in una nuova finestra di Windows Explorer.

4.6.14 Licenze

Nella sezione **Licenze** è possibile gestire le chiavi di licenza per ESET Endpoint Security e altri prodotti ESET, ad esempio ESET Remote Administrator e così via. Dopo l'acquisito, le chiavi di licenza vengono fornite insieme al nome utente e alla. Per aggiungere o rimuovere una chiave di licenza, fare clic sul pulsante **Aggiungi/Rimuovi** corrispondente della finestra di gestione licenze (**Licenze**). È possibile accedere alla gestione licenze nella struttura Configurazione avanzata facendo clic su **Strumenti** > **Licenze**.



La chiave di licenza è un file di testo contenente informazioni sul prodotto acquistato: il proprietario, il numero di licenze e la data di scadenza.

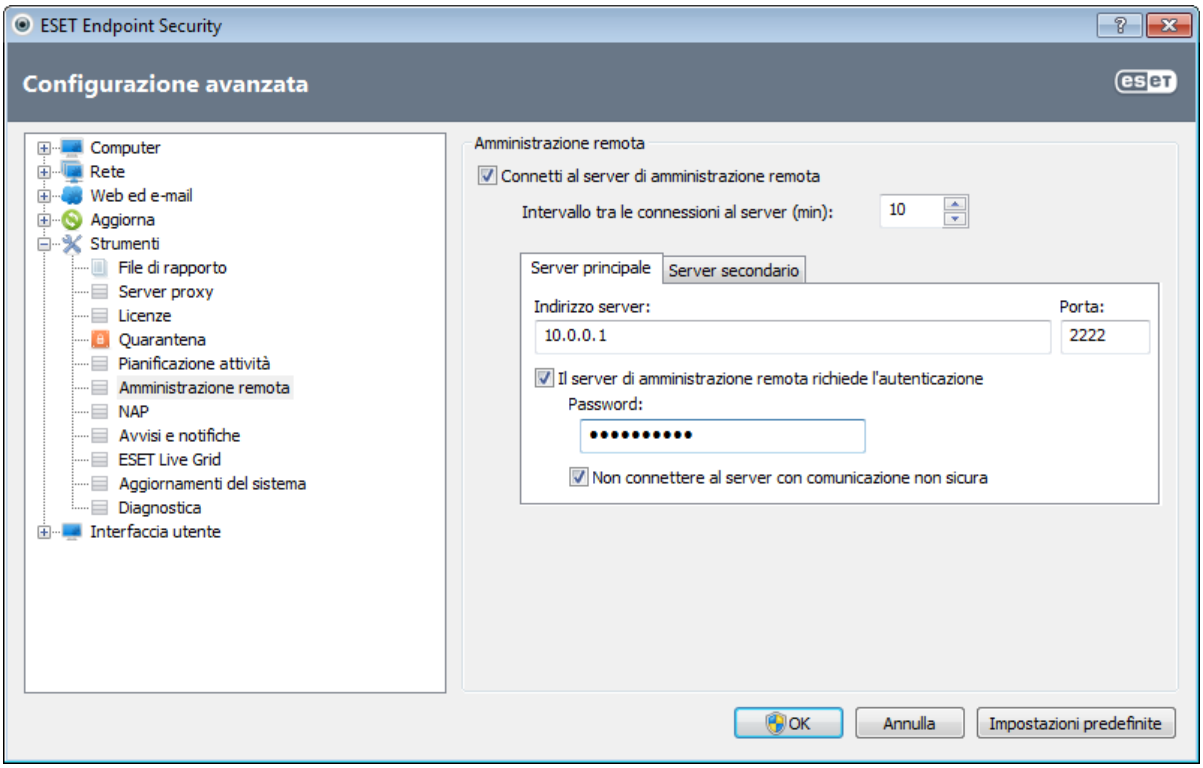
Nella finestra di gestione delle licenze è possibile caricare e visualizzare il contenuto di una chiave di licenza utilizzando il pulsante **Aggiungi...**. Le informazioni contenute vengono visualizzate nella finestra. Per eliminare un file di licenza dall'elenco, selezionarlo e fare clic su **Rimuovi**.

Se una chiave di licenza è scaduta e si desidera rinnovarla, fare clic sul pulsante **Ordina...**. Si verrà reindirizzati al negozio online.

4.6.15 Amministrazione remota

ESET Remote Administrator (ERA) è un utile strumento utilizzato per la gestione del sistema di sicurezza e per ottenere una panoramica della sicurezza globale all'interno di una rete. È particolarmente utile quando si applica a reti di una certa dimensione. ERA non solo consente di migliorare i livelli di sicurezza, ma garantisce anche una facilità di utilizzo nella gestione di ESET Endpoint Security sulle workstation client. È possibile installare, configurare, visualizzare i rapporti, pianificare attività di aggiornamento, attività di scansione e così via. La comunicazione tra ESET Remote Administrator (ERAS) e i prodotti di protezione ESET richiede la corretta configurazione di entrambi.

Le opzioni di configurazione dell'amministrazione remota sono disponibili nella schermata principale di ESET Endpoint Security. Fare clic su **Configurazione** > **Accedi a configurazione avanzata...** > **Strumenti** > **Amministrazione remota** .



Attivare l'amministrazione remota selezionando l'opzione **Connetti al server di amministrazione remota**. È possibile quindi accedere alle altre opzioni descritte di seguito:

Intervallo tra le connessioni al server (min) - Specifica la periodicità delle connessioni del prodotto di protezione ESET a ERAS per l'invio dei dati.

Server principale, Server secondario - In genere è necessario configurare solo il server principale. Se vengono eseguiti più server ERA sulla rete, può essere aggiunta un'altra connessione al server secondario ERA, il quale fungerà da soluzione di fallback. Quindi se il server principale non è accessibile, la soluzione di protezione ESET contatterà automaticamente il server secondario ERA. Contemporaneamente cercherà di ristabilire la connessione al server principale. Dopo aver riattivato la connessione, la soluzione di protezione ESET tornerà al server principale. La configurazione di due profili del server di amministrazione remoto è più adatta per i clienti mobili con client che si connettono sia dalla rete locale che dall'esterno.

Indirizzo server - Specificare il nome DNS o l'indirizzo IP del server che esegue ERAS.

Porta - Questo campo contiene la porta server predefinita utilizzata per la connessione. È consigliabile conservare l'impostazione predefinita della porta su 2222.

Intervallo tra le connessioni al server (min.) - Indica la frequenza con cui ESET Endpoint Security si connetterà a ERA Server. Se il valore impostato è 0, le informazioni vengono inviate ogni 5 secondi.

Il server di amministrazione remota richiede l'autenticazione - Consente di immettere una password per la connessione a ERA Server, se necessario.

Non connettere al server con comunicazione non sicura - Selezionare questa opzione per disattivare la connessione ai server ERA dove è attivato l'accesso non autenticato (vedere **ERA Console** > **Opzioni del server** > **Protezione** > **Attiva accesso non autenticato per client**).

Fare clic su **OK** per confermare le modifiche e applicare le impostazioni. ESET Endpoint Security utilizzerà tali impostazioni per connettersi a ERA Server.

4.7 Interfaccia utente

La sezione **Interfaccia utente** consente di configurare il comportamento dell'interfaccia grafica utente (GUI) del programma.

Tramite lo strumento Grafica, è possibile regolare l'aspetto e gli effetti del programma.

Configurando gli Avvisi e notifiche, è possibile modificare il comportamento degli avvisi sulle minacce rilevate e le notifiche di sistema in modo da adattarli alle proprie esigenze.

Se si sceglie di non visualizzare alcune notifiche, esse verranno visualizzate nell'area Finestre di notifica nascoste. In tali finestre è possibile verificarne lo stato, visualizzare ulteriori dettagli oppure rimuoverle.

Per assicurare la massima protezione del software di protezione, è possibile impedire l'esecuzione di modifiche non autorizzate proteggendo le impostazioni mediante una password tramite lo strumento Impostazione dell'accesso.

Il Menu contestuale viene visualizzato dopo aver fatto clic con il pulsante destro del mouse sull'oggetto selezionato. Utilizzare questo strumento per integrare gli elementi controllo ESET Endpoint Security nel menu contestuale.

Modalità Presentazione è utile per gli utenti che desiderano utilizzare un'applicazione senza essere interrotti dalle finestre popup, dalle attività pianificate e da qualsiasi componente che potrebbe sovraccaricare il processore e la RAM.

4.7.1 Grafica

Le opzioni di configurazione dell'interfaccia utente in ESET Endpoint Security consentono di modificare l'ambiente di lavoro per adattarlo alle esigenze specifiche dell'utente. Tali opzioni di configurazione sono disponibili nella sezione **Interfaccia utente** > **Grafica** della struttura Configurazione avanzata di ESET Endpoint Security.

Nella sezione **Elementi dell'interfaccia utente**, è necessario disattivare l'opzione **Interfaccia grafica utente** qualora gli elementi grafici rallentino le prestazioni del computer o causino altri problemi. Potrebbe inoltre essere necessario disattivare l'interfaccia grafica per gli utenti con problemi visivi in quanto potrebbe creare conflitto con determinate applicazioni utilizzate per leggere il testo visualizzato sullo schermo.

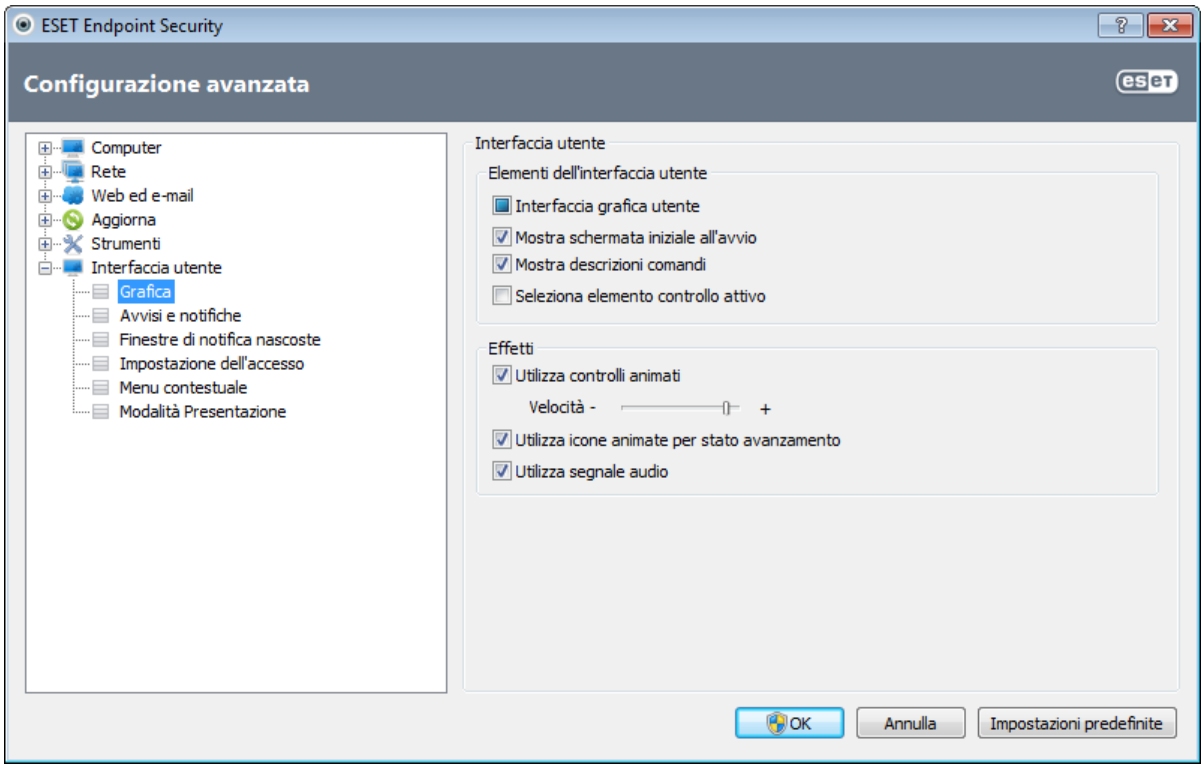
Per disattivare la schermata iniziale di ESET Endpoint Security, deselezionare l'opzione **Mostra schermata iniziale all'avvio**.

Se l'opzione **Mostra descrizioni comandi** è attivata, verrà visualizzata una breve descrizione quando si passa con il cursore sulle singole opzioni. Scegliendo l'opzione **Seleziona elemento controllo attivo**, verrà evidenziato l'elemento presente al momento nell'area attiva del cursore del mouse. Per attivare l'elemento evidenziato, fare clic su di esso.

Per aumentare o ridurre la velocità degli effetti animati, selezionare l'opzione **Utilizza controlli animati** e spostare il cursore di **Velocità** a destra o sinistra.

Per attivare l'utilizzo di icone animate per visualizzare lo stato di avanzamento di varie operazioni, selezionare l'opzione **Utilizza icone animate per stato avanzamento**.

Se si desidera che il programma emetta un suono nel caso in cui si verifichi un evento importante, selezionare **Utilizza segnale audio**. Tenere presente che il suono verrà emesso solo nel caso in cui il controllo del computer è in esecuzione o è terminato.



4.7.2 Avvisi e notifiche

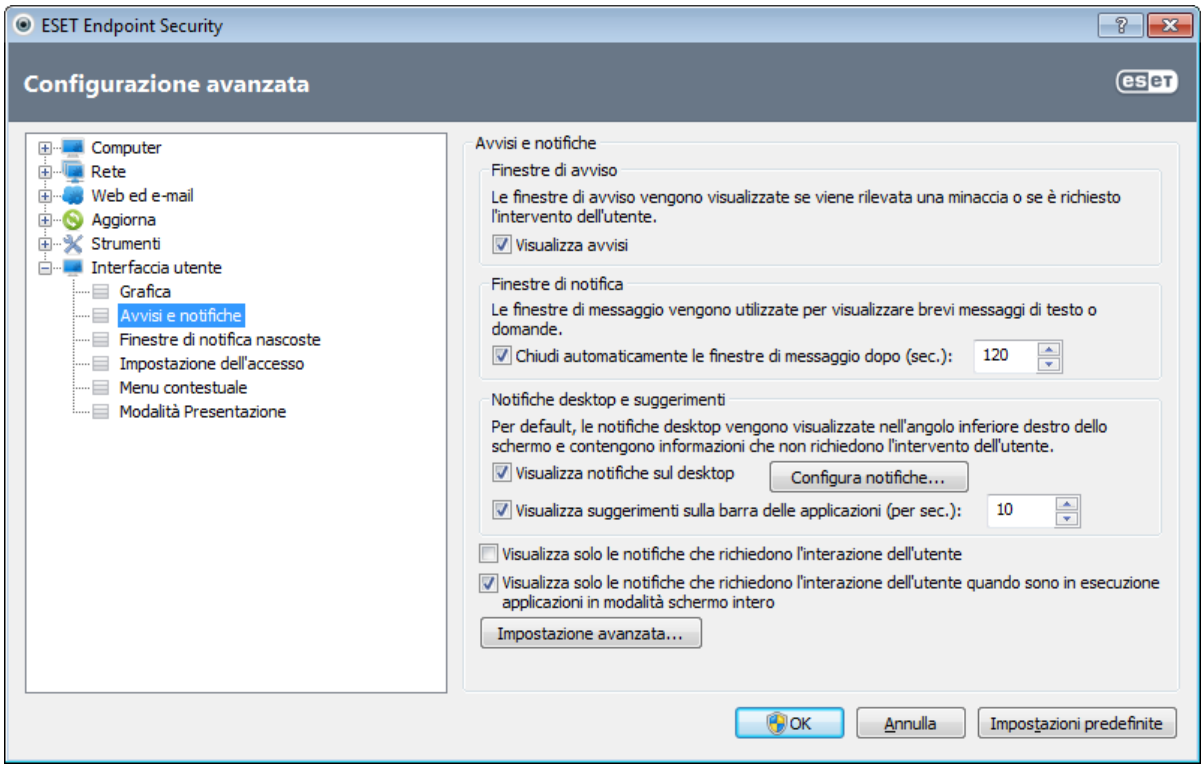
La sezione **Avvisi e notifiche** nell'**Interfaccia utente** consente di configurare la gestione dei messaggi di avviso e delle notifiche di sistema (ad esempio messaggi di aggiornamenti riusciti) in ESET Endpoint Security. È inoltre possibile impostare l'ora di visualizzazione e il livello di trasparenza delle notifiche sulla barra delle applicazioni (applicabile solo ai sistemi che supportano le notifiche sulla barra delle applicazioni).

La prima voce da considerare è **Visualizza avvisi**. Se questa opzione viene disabilitata, tutte le finestre di avviso vengono annullate. Per tale motivo, è consigliabile disattivarla solo in situazioni specifiche. Nella maggior parte dei casi, è consigliabile non modificare l'opzione predefinita (attivata).

Per chiudere automaticamente le finestre popup dopo un determinato periodo di tempo, selezionare l'opzione **Chiudi automaticamente le finestre di messaggio dopo (sec.)**. Se non vengono chiuse manualmente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il periodo di tempo specificato.

Le notifiche visualizzate sul desktop e i suggerimenti sono solo a titolo informativo e non consentono o richiedono l'interazione da parte dell'utente. Vengono visualizzati nell'area di notifica posta nell'angolo in basso a destra della schermata. Per attivare la visualizzazione delle notifiche sul desktop, selezionare l'opzione **Visualizza notifiche sul desktop**. Per modificare opzioni più dettagliate, ad esempio l'orario di visualizzazione della notifica e la trasparenza della finestra, fare clic sul pulsante **Configura notifiche...**. Per visualizzare in anteprima il funzionamento delle notifiche, fare clic sul pulsante **Anteprima**.

Per configurare la durata di visualizzazione dei suggerimenti, vedere l'opzione **Visualizza suggerimenti sulla barra delle applicazioni (per sec.)** e immettere l'intervallo di tempo desiderato nel campo adiacente.


ESET Endpoint Security
Configurazione avanzata
eset
Computer
Rete
Web ed e-mail
Aggiorna
Strumenti
Interfaccia utente
Grafica
Avvisi e notifiche
Finestre di notifica nascoste
Impostazione dell'accesso
Menu contestuale
Modalità Presentazione
Avvisi e notifiche
Finestre di avviso
Le finestre di avviso vengono visualizzate se viene rilevata una minaccia o se è richiesto l'intervento dell'utente.
Visualizza avvisi
Finestre di notifica
Le finestre di messaggio vengono utilizzate per visualizzare brevi messaggi di testo o domande.
Chiudi automaticamente le finestre di messaggio dopo (sec.):
120
Notifiche desktop e suggerimenti
Per default, le notifiche desktop vengono visualizzate nell'angolo inferiore destro dello schermo e contengono informazioni che non richiedono l'intervento dell'utente.
Visualizza notifiche sul desktop
Configura notifiche...
Visualizza suggerimenti sulla barra delle applicazioni (per sec.):
10
Visualizza solo le notifiche che richiedono l'interazione dell'utente
Visualizza solo le notifiche che richiedono l'interazione dell'utente quando sono in esecuzione applicazioni in modalità schermo intero
Impostazione avanzata...
OK
Annulla
Impostazioni predefinite

L'opzione **Visualizza solo le notifiche che richiedono l'interazione dell'utente** consente di attivare/disattivare la visualizzazione di avvisi e notifiche che non richiedono l'intervento da parte dell'utente. Selezionare **Visualizza solo le notifiche che richiedono l'interazione dell'utente quando sono in esecuzione applicazioni in modalità schermo intero** per eliminare tutte le notifiche non interattive.

Fare clic su **Impostazione avanzata...** per accedere a ulteriori opzioni di configurazione degli **Avvisi e notifiche**.

4.7.2.1 Configurazione avanzata

Nel menu a discesa **Livello di dettaglio minimo degli eventi da visualizzare** è possibile selezionare il livello iniziale di gravità degli avvisi e delle notifiche da visualizzare.

- **Diagnostica** - Registra tutte le informazioni necessarie per l'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativi** - Messaggi di record informativi che includono gli aggiornamenti riusciti e tutti i record indicati in precedenza.
- **Allarmi** - Consente di registrare errori critici e messaggi di allarme.
- **Errori** - Verranno registrati errori quali "Errore durante il download del file" ed errori critici.
- **Critici** - Registra solo gli errori critici (errore che avvia la protezione antivirus, il Firewall personalee così via).

L'ultima funzione in questa sezione consente di configurare la destinazione delle notifiche in un ambiente multi-utente. Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente** viene specificato l'utente che riceverà le notifiche di sistema e di altro tipo sui sistemi che consentono la connessione simultanea di più utenti. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, a condizione che tutte le notifiche di sistema vengano inviate all'amministratore.

4.7.3 Finestre di notifica nascoste

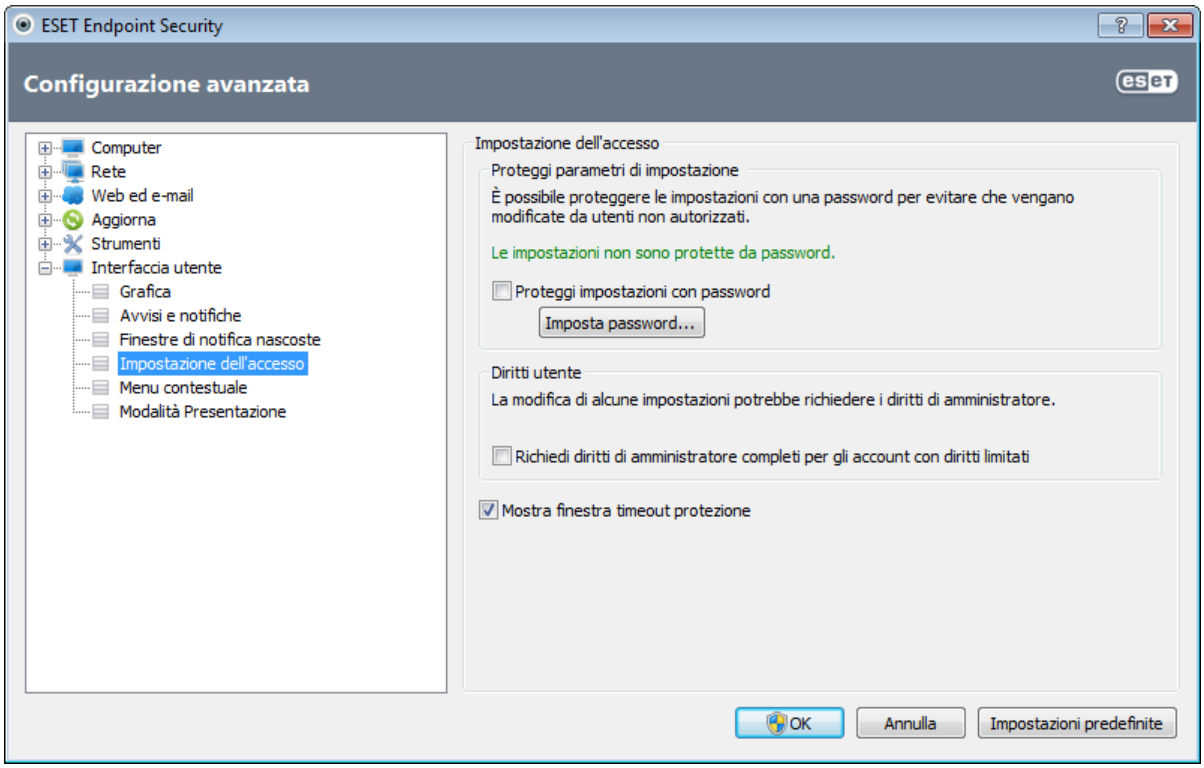
Se per le finestre di notifica (avvisi) visualizzate in precedenza è stata selezionata l'opzione **Non visualizzare più questo messaggio**, questa verrà visualizzata nell'elenco delle finestre di notifica nascoste. Le azioni eseguite automaticamente vengono visualizzate nella colonna **Conferma**.

Mostra - Mostra un'anteprima delle finestre di notifica al momento non visualizzate e per le quali è configurata un'azione automatica.

Rimuovi - Rimuove voci dall'elenco **Finestre di messaggio nascoste**. Tutte le finestre di notifica rimosse dall'elenco verranno visualizzate nuovamente.

4.7.4 Configurazione dell'accesso

Per garantire la massima sicurezza del sistema è fondamentale che ESET Endpoint Security sia configurato correttamente. Qualsiasi modifica non appropriata potrebbe causare la perdita di dati importanti. L'opzione è disponibile nel sottomenu **Impostazione dell'accesso** nell'**Interfaccia utente** della struttura Configurazione avanzata. Per evitare modifiche non autorizzate, i parametri di impostazione di ESET Endpoint Security possono essere protetti con password.



Proteggi impostazioni con password - Blocca/sblocca i parametri di impostazione del programma. Selezionare o deselezionare la casella di controllo per aprire la finestra di impostazione della password.

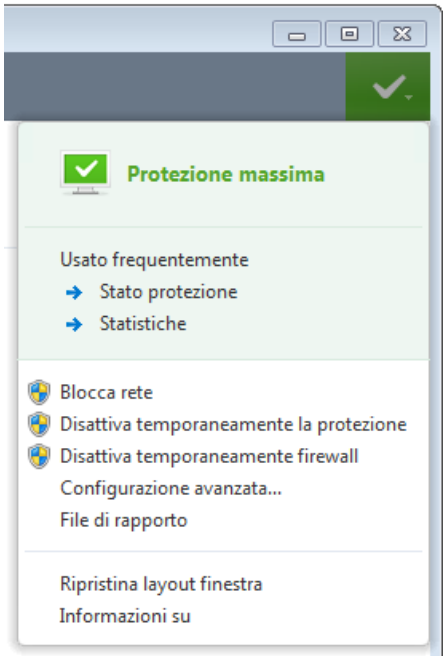
Per impostare o modificare una password per proteggere i parametri di configurazione, fare clic su **Imposta password...**.

Richiedi diritti di amministratore completi per gli account con diritti limitati - Selezionare questa opzione per richiedere all'utente corrente (nel caso non disponga dei diritti di amministratore) di immettere nome utente e password per la modifica di alcuni parametri del sistema (analogo a Controllo dell'account utente in Windows Vista). Tali modifiche includono la disattivazione dei moduli di protezione o del firewall.

Mostra finestra timeout protezione - Se questa opzione è selezionata, verrà visualizzata questa richiesta quando si disattiva temporaneamente la protezione dal menu del programma o dalla sezione **ESET Endpoint Security** > **Configura**. Un menu a comparsa **Intervallo di tempo** nella finestra **Disattiva temporaneamente la protezione** indica l'intervallo di tempo durante il quale tutte le parti selezionate della protezione saranno disattivate.

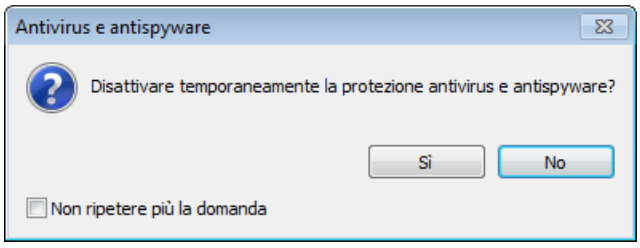
4.7.5 Menu del programma

Il menu del programma principale contiene alcune delle funzioni e delle opzioni di impostazione più importanti.

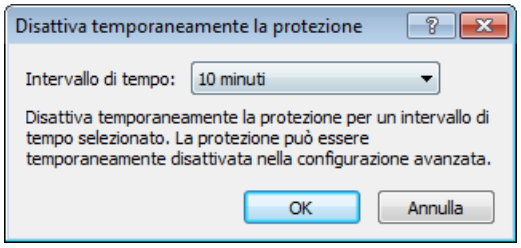


Usato frequentemente - Consente di visualizzare le parti di ESET Endpoint Security che vengono utilizzate più frequentemente. È possibile accedervi rapidamente dal menu del programma.

Disattiva temporaneamente la protezione - Visualizza la finestra di dialogo di conferma che consente di disattivare la Protezione antivirus e antispyware che protegge da attacchi dannosi al sistema controllando file e comunicazioni Web ed e-mail. Selezionare la casella di controllo **Non ripetere più la domanda** per non visualizzare più questo messaggio.



Il menu a discesa **Intervallo di tempo** rappresenta l'intervallo di tempo durante il quale la Protezione antivirus e antispyware verrà disattivata.


Disattiva temporaneamente la protezione
Intervallo di tempo:
10 minuti
Disattiva temporaneamente la protezione per un intervallo di tempo selezionato. La protezione può essere temporaneamente disattivata nella configurazione avanzata.
OK
Annulla

Blocca rete - Il Firewall personale bloccherà tutto il traffico Internet e di rete in uscita/in entrata.

Disattiva temporaneamente firewall - Imposta il firewall su uno stato non attiva. Per ulteriori informazioni, consultare il capitolo Integrazione nel sistema del Firewall personale.

Configurazione avanzata... - Selezionare questa opzione per accedere alla struttura **Configurazione avanzata**. È possibile accedere a tale struttura anche in altri modi, ad esempio premendo il tasto F5 oppure accedendo a **Configurazione** > **Accedi a configurazione avanzata...**.

File di rapporto - I File di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate.

Ripristina layout finestra - Ripristina le dimensioni predefinite e la posizione sullo schermo della finestra di ESET Endpoint Security.

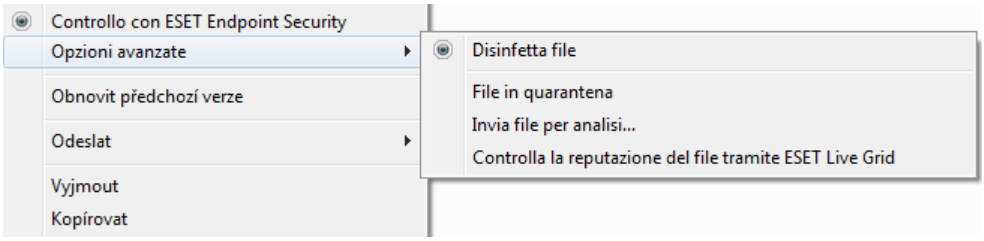
Informazioni su - Vengono fornite informazioni sul sistema, dettagli sulla versione installata di ESET Endpoint Security e sui relativi moduli di programma installati. È inoltre disponibile la data di scadenza della licenza. Alla fine, sono visualizzate le informazioni sul sistema operativo e sulle risorse di sistema.

4.7.6 Menu contestuale

Il menu contestuale viene visualizzato dopo aver fatto clic con il pulsante destro del mouse sull'oggetto selezionato. Nel menu sono elencate tutte le opzioni disponibili da eseguire sull'oggetto.

È possibile integrare gli elementi controllo ESET Endpoint Security nel menu contestuale. Sono disponibili opzioni di configurazione più dettagliate per questa funzionalità nella struttura Configurazione avanzata in **Interfaccia utente** > **Menu contestuale**.

Integra nel menu contestuale - Integrare gli elementi controllo ESET Endpoint Security nel menu contestuale.



Nel menu a discesa **Tipo di menu** sono disponibili le seguenti opzioni:

- **Completo (Esegui prima scansione)** - Attiva tutte le opzioni del menu contestuale. Nel menu principale verrà visualizzata l'opzione **Controllo con ESET Endpoint Security**.
- **Completo (Esegui prima pulitura)** - Attiva tutte le opzioni del menu contestuale. Nel menu principale verrà visualizzata l'opzione **Pulisci con ESET Endpoint Security**.
- **Solo scansione** - Nel menu contestuale verrà visualizzata solo l'opzione **Controllo con ESET Endpoint Security**.
- **Solo pulitura** - Nel menu contestuale verrà visualizzata solo l'opzione **Pulisci con ESET Endpoint Security**.

4.7.7 Modalità Presentazione

Modalità Presentazione è una funzionalità per gli utenti che desiderano utilizzare il software senza essere interrotti, che non desiderano essere disturbati dalle finestre popup e che desiderano ridurre al minimo l'utilizzo della CPU. Modalità Presentazione può essere utilizzata anche durante le presentazioni che non possono essere interrotte dall'attività antivirus. Attivando tale funzionalità, tutte le finestre popup sono disattivate e l'attività di Pianificazione attività sarà completamente interrotta. La protezione del sistema è ancora in esecuzione in background ma non richiede alcun intervento da parte dell'utente.

È possibile attivare o disattivare la Modalità Presentazione nella finestra principale del programma facendo clic su **Configurazione** > **Computer**, quindi su **Attiva** in **Modalità Presentazione** nella struttura Configurazione avanzata (F5) espandendo **Interfaccia utente**, facendo clic su **Modalità Presentazione** e selezionando la casella di controllo accanto a **Attiva Modalità Presentazione**. L'attivazione della Modalità Presentazione rappresenta un potenziale rischio per la protezione. Per tale motivo, l'icona relativa allo stato della protezione sulla barra delle attività diventa di colore arancione e viene visualizzato un avviso. Questo avviso verrà inoltre visualizzato nella finestra principale del programma dove Modalità Presentazione attivata in arancione.

Se si seleziona la casella di controllo **Attiva Modalità Presentazione quando vengono eseguite automaticamente applicazioni in modalità a schermo intero**, la Modalità Presentazione verrà avviata automaticamente dopo aver avviato un'applicazione in modalità a schermo intero e verrà interrotta quando si esce dall'applicazione. Questa funzionalità risulta particolarmente utile per avviare la Modalità Presentazione subito dopo aver avviato un gioco, aver aperto un'applicazione in modalità a schermo intero o aver avviato una presentazione.

È inoltre possibile selezionare la casella di controllo **Disattiva automaticamente Modalità Presentazione dopo X minuti** per definire l'intervallo di tempo (il valore predefinito è 1 minuto). Questa opzione è utile quando è necessario attivare la Modalità Presentazione solo per un intervallo di tempo specifico e si desidera disattivarla successivamente.

NOTA: Se il Firewall è in modalità interattiva e la Modalità Presentazione è attivata, si potrebbero riscontrare problemi di connessione a Internet. Ciò potrebbe causare problemi se si inizia un gioco che necessita della connessione a Internet. In genere verrebbe richiesto di confermare tale azione (se non sono state definite regole o eccezioni di comunicazione) ma l'interazione da parte dell'utente è disattivata nella Modalità Presentazione. Per ovviare al problema, è necessario definire una regola di comunicazione per ogni applicazione che potrebbe entrare in conflitto con questo comportamento o utilizzare una Modalità di filtro differente nel Firewall personale. Tenere inoltre presente che se la Modalità Presentazione è attivata e si accede a una pagina Web o a un'applicazione che potrebbe rappresentare un

rischio per la sicurezza, potrebbe essere bloccata ma non verrà visualizzato alcun avviso o notifica in quanto l'interazione utente è disattivata.

5. Utente avanzato

5.1 Configurazione del server proxy

Nelle reti LAN di grandi dimensioni, la connessione del computer dell'utente a Internet può essere mediata da un server proxy. In questo caso, occorre definire le impostazioni seguenti. In caso contrario, il programma non sarà in grado di aggiornarsi automaticamente. In ESET Endpoint Security, il server proxy può essere configurato in due sezioni differenti della struttura Configurazione avanzata.

Le impostazioni del server proxy possono innanzitutto essere configurate in **Configurazione avanzata** da **Strumenti** > **Server proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per l'intera applicazione ESET Endpoint Security. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy a questo livello, selezionare la casella di controllo **Usa server proxy**, quindi immettere l'indirizzo del server proxy nel campo **Server proxy**, insieme al numero di **Porta** del server proxy.

Se per la comunicazione con il server proxy è necessaria l'autenticazione, selezionare la casella di controllo **Il server proxy richiede l'autenticazione** e immettere **Nome utente** e **Password** validi nei rispettivi campi. Fare clic sul pulsante **Rileva server proxy** per rilevare e popolare automaticamente le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer.

NOTA: questa funzione non consente di recuperare i dati sull'autenticazione (nome utente e password). Tali informazioni devono quindi essere immesse dall'utente.

Le impostazioni del server proxy possono inoltre essere definite nell'ambito dell'impostazione aggiornamento avanzata (sezione **Aggiorna** della struttura di **Configurazione avanzata**). Questa impostazione è applicabile al profilo di aggiornamento fornito ed è consigliata sui notebook che ricevono spesso aggiornamenti delle firme antivirali da diverse postazioni. Per ulteriori informazioni su questa impostazione, consultare la sezione Impostazione aggiornamento avanzata.

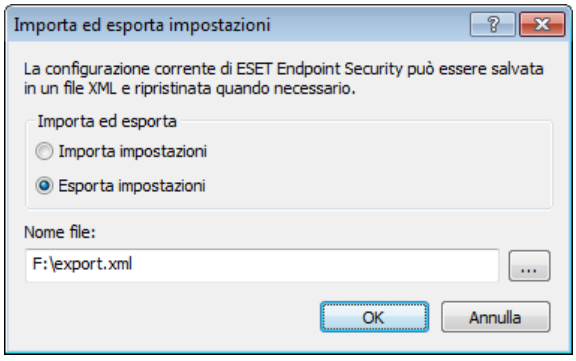
5.2 Importa ed esporta impostazioni

Le configurazioni di importazione ed esportazione di ESET Endpoint Security sono disponibili in **Configurazione**.

Le opzioni di importazione e di esportazione utilizzano entrambe il tipo di file .xml. Le opzioni di importazione e di esportazione sono utili nel caso in cui si desideri effettuare il backup della configurazione corrente di ESET Endpoint Security per poterlo utilizzare in un secondo momento. L'opzione di esportazione delle impostazioni è utile anche per gli utenti che desiderano utilizzare la configurazione preferita di ESET Endpoint Security su più sistemi. In tal modo, sarà infatti possibile importare facilmente un file XML per il trasferimento delle impostazioni desiderate.

L'importazione della configurazione è molto semplice. Nella finestra principale del programma, fare clic su **Configurazione** > **Importa ed esporta impostazioni...** quindi selezionare l'opzione **Importa impostazioni**. Inserire il percorso del file di configurazione o fare clic sul pulsante **...** per ricercare il file di configurazione che si desidera importare.

Le operazioni per esportare una configurazione sono molto simili. Nella finestra principale del programma, fare clic su **Configurazione** > **Importa ed esporta impostazioni...** Selezionare l'opzione **Esporta impostazioni** e immettere il **Nome file** del file di configurazione (ad esempio export.xml). Utilizzare il browser per selezionare un percorso sul computer in cui salvare il file di configurazione.



5.3 Tasti di scelta rapida

I tasti di scelta rapida che possono essere utilizzati con ESET Endpoint Security includono:

Ctrl+G	disattiva l'interfaccia utente nel prodotto
Ctrl+I	apre la pagina ESET SysInspector
Ctrl+L	apre la pagina File di rapporto
Ctrl+S	apre la pagina Pianificazione attività
Ctrl+Q	apre la pagina Quarantena
Ctrl+U	apre una finestra di dialogo dove è possibile impostare il nome utente e la password
Ctrl+R	ripristina le dimensioni predefinite e la posizione sullo schermo della finestra

Per una migliore navigazione all'interno del prodotto di protezione ESET è possibile utilizzare i seguenti tasti di scelta rapida:

F1	apre le pagine della Guida
F5	apre la schermata Configurazione avanzata
Tasti Su/Giù	navigazione all'interno delle voci del prodotto
*	ingrandisce il nodo della struttura Configurazione avanzata
-	riduce a icona il nodo della struttura Configurazione avanzata
TAB	sposta il cursore in una finestra
Esc	chiude la finestra di dialogo attiva

5.4 Riga di comando

Il modulo antivirus di ESET Endpoint Security può essere avviato dalla riga di comando, manualmente con il comando "ecls" oppure con un file batch ("bat"). Utilizzo dello scanner della riga di comando ESET:

```
ecls [OPTIONS..] FILES..
```

È possibile utilizzare i parametri e le opzioni riportati di seguito quando viene eseguita una scansione su richiesta dalla riga di comando:

Opzioni

/base-dir=FOLDER	carica moduli da CARTELLA
/quar-dir=FOLDER	CARTELLA di quarantena
/exclude=MASK	escludi dalla scansione i file corrispondenti a MASCHERA
/subdir	esegui controllo delle sottocartelle (impostazione predefinita)
/no-subdir	non eseguire controllo delle sottocartelle
/max-subdir-level=LEVEL	sottolivello massimo delle cartelle all'interno di cartelle su cui eseguire la scansione
/symlink	segui i collegamenti simbolici (impostazione predefinita)
/no-symlink	ignora collegamenti simbolici
/ads	esegui la scansione di ADS (impostazione predefinita)
/no-ads	non eseguire la scansione di ADS
/log-file=FILE	registra output nel FILE
/log-rewrite	sovrascrivi il file di output (impostazione predefinita: aggiungi)
/log-console	registra l'output nella console (impostazione predefinita)
/no-log-console	non registrare l'output nella console
/log-all	registra anche file puliti
/no-log-all	non registrare file puliti (impostazione predefinita)
/aind	mostra indicatore di attività
/auto	controlla e disinfetta automaticamente tutti i dischi locali

Opzioni scanner

/files	esegui controllo dei file (impostazione predefinita)
/no-files	non eseguire controllo dei file
/memory	esegui scansione della memoria
/boots	esegui la scansione dei settori di avvio
/no-boots	non eseguire la scansione dei settori di avvio (impostazione predefinita)
/arch	esegui controllo degli archivi (impostazione predefinita)
/no-arch	non eseguire controllo degli archivi

/max-obj-size=SIZE	esegui solo la scansione dei file inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/max-arch-level=LEVEL	sottolivello massimo degli archivi all'interno di archivi (archivi nidificati) su cui eseguire la scansione
/scan-timeout=LIMIT	esegui scansione degli archivi per LIMITE secondi al massimo
/max-arch-size=SIZE	esegui la scansione dei file di un archivio solo se inferiori a DIMENSIONE (impostazione predefinita 0 = illimitato)
/max-sfx-size=SIZE	esegui la scansione dei file di un archivio autoestraente solo se inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/mail	esegui la scansione dei file di e-mail (impostazione predefinita)
/no-mail	non eseguire controllo dei file di e-mail
/mailbox	esegui la scansione delle caselle di posta (impostazione predefinita)
/no-mailbox	non eseguire la scansione delle caselle di posta
/sfx	esegui la scansione degli archivi autoestraenti (impostazione predefinita)
/no-sfx	non eseguire controllo degli archivi autoestraenti
/rtp	esegui la scansione degli eseguibili compressi (impostazione predefinita)
/no-rtp	non eseguire la scansione degli eseguibili compressi
/adware	esegui la scansione di Adware/Spyware/Riskware (impostazione predefinita)
/no-adware	non eseguire la scansione di Adware/Spyware/Riskware
/unsafe	esegui la scansione delle applicazioni potenzialmente pericolose
/no-unsafe	non eseguire la scansione delle applicazioni potenzialmente pericolose (impostazione predefinita)
/unwanted	esegui la scansione delle applicazioni potenzialmente indesiderate
/no-unwanted	non eseguire la scansione delle applicazioni potenzialmente indesiderate (impostazione predefinita)
/pattern	utilizza le firme digitali (impostazione predefinita)
/no-pattern	non utilizzare le firme digitali
/heur	attiva l'euristica (impostazione predefinita)
/no-heur	disattiva l'euristica
/adv-heur	attiva l'euristica avanzata (impostazione predefinita)
/no-adv-heur	disattiva l'euristica avanzata
/ext=EXTENSIONS	esegui scansione solo di ESTENSIONI delimitate da due punti
/ext-exclude=EXTENSIONS	escludi dal controllo le ESTENSIONI delimitate da due punti
/clean-mode=MODE	utilizza la MODALITÀ pulitura per gli oggetti infetti. Opzioni disponibili: nessuna, standard (valore predefinito), massima, rigorosa, eliminazione
/quarantena	copiare i file infettati (se puliti) in Quarantena (integra l'azione eseguita durante la pulizia)
/no-quarantena	non copiare file infettati in Quarantena

Opzioni generali

/help	mostra guida ed esci
/version	mostra informazioni sulla versione ed esci
/preserve-time	mantieni timestamp dell'ultimo accesso

Codici di uscita

0	nessuna minaccia rilevata
1	minaccia rilevata e pulita
10	impossibile controllare alcuni file (potrebbero essere minacce)
50	trovata minaccia
100	errore

NOTA: i codici di uscita superiori a 100 indicano che non è stata eseguita la scansione del file, il quale potrebbe quindi essere infetto.

5.5 ESET SysInspector

5.5.1 Introduzione a ESET SysInspector

L'applicazione ESET SysInspector ispeziona il computer in modo approfondito e visualizza i dati raccolti in modo globale. La raccolta di informazioni su driver e applicazioni, su connessioni di rete o importanti voci di registro semplifica il controllo di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

È possibile accedere a ESET SysInspector in due modi: dalla versione integrata nelle soluzioni ESET Security o scaricando gratuitamente la versione indipendente (SysInspector.exe) dal sito Web ESET. Le funzionalità e i comandi di entrambe le versioni sono identici. L'unica differenza consiste nella gestione dei risultati. La versione indipendente e quella integrata consentono entrambe di esportare snapshot del sistema su un file XML e salvarli su disco. La versione integrata consente tuttavia anche di memorizzare gli snapshot di sistema direttamente in **Strumenti** > **ESET SysInspector** (tranne ESET Remote Administrator).

È necessario attendere qualche minuto per consentire a ESET SysInspector di controllare il computer. A seconda della configurazione hardware, del sistema operativo e del numero di applicazioni installate nel computer in uso, questa operazione potrebbe richiedere da 10 secondi ad alcuni minuti.

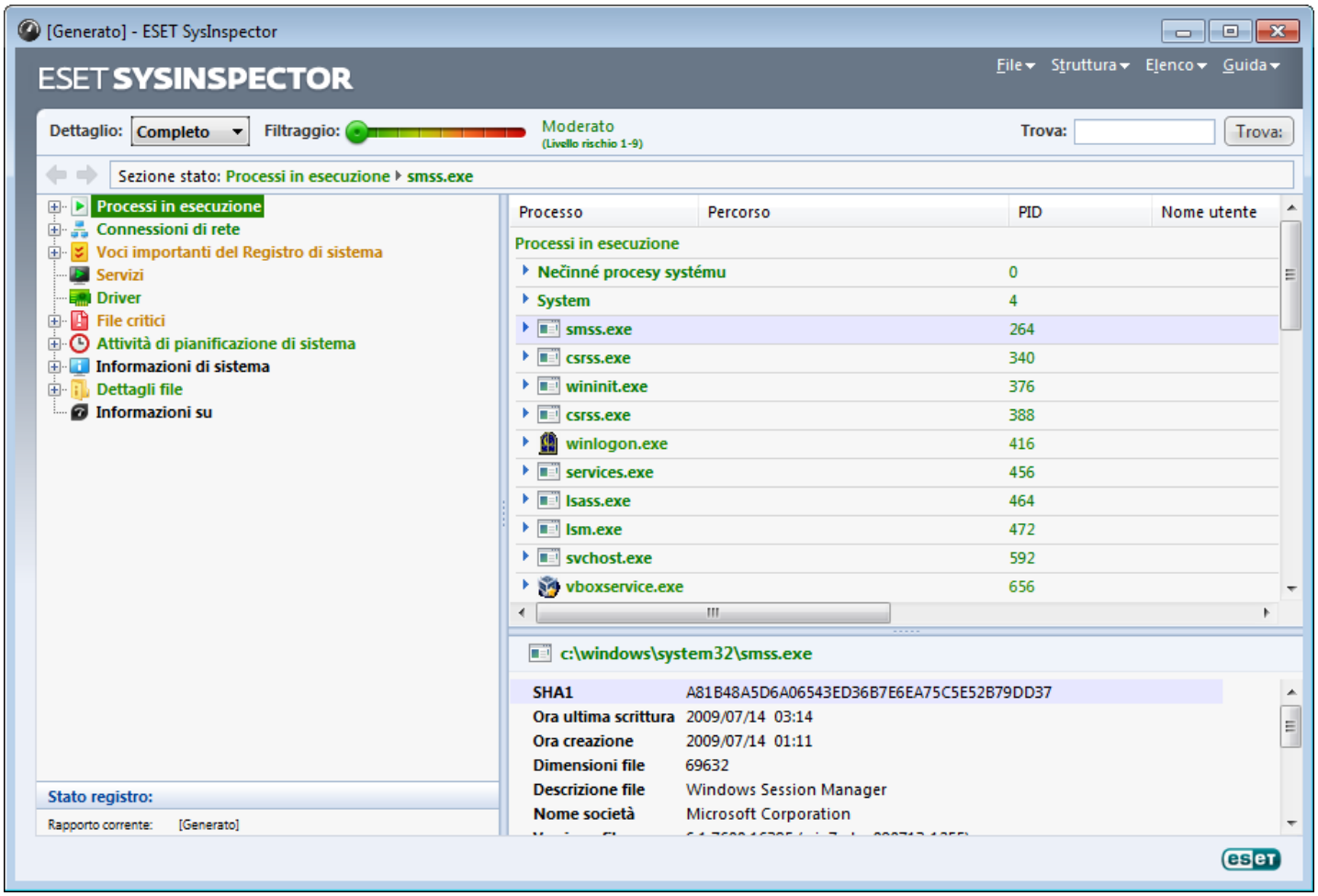
5.5.1.1 Avvio di ESET SysInspector

Per avviare ESET SysInspector è sufficiente eseguire il file eseguibile SysInspector.exe scaricato dal sito Web ESET.

È necessario attendere che l'applicazione abbia esaminato il sistema in uso. Questa operazione potrebbe richiedere diversi minuti a seconda dell'hardware e dei dati raccolti.

5.5.2 Interfaccia utente e utilizzo dell'applicazione

Per chiarezza, la finestra principale è stata divisa in quattro sezioni principali: i comandi del programma sono posizionati nella parte superiore della finestra; a sinistra viene visualizzata la finestra di spostamento, a destra, nella parte centrale, è disponibile la finestra Descrizione e, infine, nella parte inferiore destra della schermata viene visualizzata la finestra Dettagli. Nella sezione Stato registro sono elencati i parametri principali di un rapporto (filtro usato, tipo di filtro, se il rapporto è il risultato di un confronto e così via).



5.5.2.1 Comandi del programma

La presente sezione contiene la descrizione di tutti i comandi del programma disponibili in ESET SysInspector.

File

Selezionare **File** per memorizzare lo stato attuale del sistema per un'analisi futura oppure aprire un rapporto precedentemente archiviato. Ai fini della pubblicazione, è consigliabile generare un rapporto **Idoneo all'invio**. In questo formato, nel rapporto vengono omesse informazioni riservate (nome utente attuale, nome computer, nome dominio, privilegi utente attuale, variabili d'ambiente e così via).

NOTA: è possibile aprire i rapporti di ESET SysInspector precedentemente archiviati trascinandoli nella finestra principale.

Struttura

Consente di espandere o chiudere tutti i nodi e di esportare le sezioni selezionate sullo script di servizio.

Elenco

Contiene funzioni per uno spostamento più pratico all'interno del programma e varie altre funzioni, ad esempio la ricerca di informazioni su Internet.

Guida

Contiene informazioni sull'applicazione e sulle relative funzioni.

Dettaglio

Questa impostazione influenza le informazioni visualizzate nella finestra principale al fine di semplificarne l'utilizzo. Nella modalità "Base" si ha accesso alle informazioni utilizzate per trovare soluzioni a problemi comuni del sistema. Nella modalità "Media" il programma visualizza i dettagli meno utilizzati, mentre nella modalità "Completa", ESET SysInspector mostra tutte le informazioni necessarie alla soluzione di problemi specifici.

Filtraggio elementi

Il filtraggio elementi viene utilizzato soprattutto per individuare file o voci di registro sospetti all'interno del sistema. Regolando il cursore, è possibile filtrare gli elementi in base al livello di rischio. Se il cursore si trova all'estrema sinistra (Livello di rischio 1) vengono visualizzati tutti gli elementi. Spostando il cursore a destra, il programma esclude tutti gli elementi meno rischiosi rispetto al livello di rischio attuale, visualizzando solo gli elementi che risultano più sospetti del livello visualizzato. Quando il cursore si trova all'estrema destra, il programma visualizza solo gli elementi dannosi conosciuti.

Tutti gli elementi contrassegnati con un livello di rischio compreso tra 6 e 9 rappresentano un rischio per la sicurezza. Se ESET SysInspector ha rilevato un elemento di questo tipo, si consiglia di eseguire la scansione del sistema con ESET Online Scanner, se non si utilizzano alcune delle soluzioni di protezione di ESET. ESET Online Scanner è un servizio gratuito.

NOTA: il Livello di rischio di un elemento può essere determinato rapidamente confrontandone il colore con quello del cursore Livello di rischio.

Ricerca

L'opzione Cerca può essere utilizzata per individuare rapidamente un elemento specifico in base al nome o parte di esso. I risultati della richiesta di ricerca vengono visualizzati nella finestra Descrizione.

Ritorna

Facendo clic sulla freccia indietro o avanti è possibile tornare alle informazioni precedentemente visualizzate nella finestra Descrizione. Utilizzare i tasti Cancella e Barra spaziatrice anziché fare clic avanti e indietro all'interno del programma.

Sezione stato

Visualizza il nodo corrente nella finestra di spostamento.

Importante: gli elementi evidenziati in rosso sono sconosciuti. Per tale motivo, il programma li segna come potenzialmente pericolosi. Se un elemento è segnalata in rosso, non significa automaticamente che sia possibile eliminare il file. Prima di procedere all'eliminazione, assicurarsi che i file siano effettivamente pericolosi o non necessari.

5.5.2.2 Navigare in ESET SysInspector

ESET SysInspector divide vari tipi di informazioni in numerose sezioni di base, dette nodi. Se disponibili, ulteriori dettagli saranno visualizzabili espandendo ciascun nodo nei relativi sottonodi. Per espandere o comprimere un nodo, fare doppio clic sul nome del nodo o, in alternativa, selezionare + o − accanto al nome del nodo. Spostandosi nella struttura ad albero di nodi e sottonodi della finestra di spostamento, sono disponibili vari dettagli su ciascun nodo presente nella finestra Descrizione. Navigando tra gli elementi della finestra Descrizione, è possibile visualizzare ulteriori dettagli per ciascun elemento nella finestra Dettagli.

Di seguito vengono riportate le descrizioni dei nodi principali presenti nella finestra di spostamento e le relative informazioni delle finestre Descrizione e Dettagli.

Processi in esecuzione

Questo nodo contiene informazioni sulle applicazioni e sui processi in esecuzione durante la generazione del rapporto. Nella finestra Descrizione sono disponibili dettagli aggiuntivi su ciascun processo, ad esempio le librerie dinamiche utilizzate dal processo e la loro posizione nel sistema, il nome del produttore dell'applicazione e il livello di rischio del file.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

NOTA: un sistema operativo è basato su diversi componenti kernel, in esecuzione 24 ore su 24, 7 giorni su 7, che forniscono funzioni fondamentali e di base per le altre applicazioni utente. In alcuni casi, tali processi sono visualizzati nello strumento ESET SysInspector con il percorso file preceduto da \??\. Quei simboli forniscono un'ottimizzazione per i processi in questione prima di avviarli e risultano sicuri per il sistema.

Connessioni di rete

La finestra Descrizione contiene un elenco di processi e applicazioni che comunicano sulla rete utilizzando il protocollo selezionato nella finestra di spostamento (TCP o UDP), unitamente all'indirizzo remoto a cui è collegata l'applicazione. È inoltre possibile verificare gli indirizzi IP dei server DNS.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

Voci importanti del Registro di sistema

Contiene un elenco delle voci di registro selezionate che sono spesso correlate a vari problemi del sistema, ad esempio quelle indicano i programmi di avvio, oggetti browser helper (BHO) e così via.

Nella finestra Descrizione è possibile visualizzare i file correlati a voci di registro specifiche. Nella finestra Dettagli è possibile visualizzare maggiori informazioni.

Servizi

La finestra Descrizione contiene un elenco di file registrati come Servizi Windows. Nella finestra Dettagli è possibile controllare il modo in cui è impostato l'avvio del servizio insieme ai dettagli specifici del file.

Driver

Un elenco di driver installati nel sistema.

File critici

Nella finestra Descrizione è visualizzato il contenuto dei file critici relativi al sistema operativo Microsoft Windows.

Attività di pianificazione di sistema

Contiene un elenco delle attività avviate dall'Utilità di pianificazione di Windows a un orario/intervallo specificato.

Informazioni di sistema

Contiene informazioni dettagliate sull'hardware e sul software, oltre a informazioni sulle variabili d'ambiente impostate, sui diritti utente e sui rapporti eventi di sistema.

Dettagli file

Un elenco di file di sistema importanti e di file presenti nella cartella Programmi. Per maggiori informazioni sui file in questione, fare riferimento alle finestre Descrizione e Dettagli.

Informazioni su

Informazioni sulla versione di ESET SysInspector ed elenco dei moduli del programma.

5.5.2.2.1 Tasti di scelta rapida

I tasti di scelta rapida che possono essere utilizzati con ESET SysInspector includono:

File

Ctrl+O	apre il rapporto esistente
Ctrl+S	salva i rapporti creati

Genera

Ctrl+G	genera uno snapshot di stato computer standard
Ctrl+H	genera uno snapshot di stato computer che potrebbe registrare anche informazioni sensibili

Filtraggio elementi

1, O	non a rischio, visualizzati gli elementi con livello di rischio 1-9
2	non a rischio, visualizzati gli elementi con livello di rischio 2-9
3	non a rischio, visualizzati gli elementi con livello di rischio 3-9
4, U	sconosciuto, visualizzati gli elementi con livello di rischio 4-9
5	sconosciuto, visualizzati gli elementi con livello di rischio 5-9
6	sconosciuto, visualizzati gli elementi con livello di rischio 6-9
7, B	a rischio, visualizzati gli elementi con livello di rischio 7-9

8	a rischio, visualizzati gli elementi con livello di rischio 8-9
9	a rischio, visualizzati gli elementi con livello di rischio 9
-	diminuisce il livello di rischio
+	aumenta il livello di rischio
Ctrl+9	modalità di filtraggio, livello uguale o più alto
Ctrl+O	modalità di filtraggio, solo livello uguale

Visualizza

Ctrl+5	visualizza per fornitore, tutti i fornitori
Ctrl+6	visualizza per fornitore, solo Microsoft
Ctrl+7	visualizza per fornitore, tutti gli altri fornitori
Ctrl+3	mostra tutti i dettagli
Ctrl+2	livello di dettaglio medio
Ctrl+1	visualizzazione di base
Cancella	indietro di un passaggio
Barra spaziatrice	avanti di un passaggio
Ctrl+W	espande la struttura
Ctrl+Q	comprime la struttura

Altri comandi

Ctrl+T	va alla posizione originale dell'elemento dopo averlo selezionato nei risultati di ricerca
Ctrl+P	visualizza informazioni di base su un elemento
Ctrl+A	visualizza informazioni complete di un elemento
Ctrl+C	copia la struttura dell'elemento attuale
Ctrl+X	copia gli elementi
Ctrl+B	trova su Internet le informazioni sui file selezionati
Ctrl+L	apre la cartella dove si trova il file selezionato
Ctrl+R	apre la voce corrispondente nell'editor del Registro di sistema
Ctrl+Z	copia un percorso di un file (se l'elemento è relativo a un file)
Ctrl+F	passa al campo di ricerca
Ctrl+D	chiude i risultati di ricerca
Ctrl+E	esegue lo script di servizio

Confronto

Ctrl+Alt+O	apre il rapporto originale/comparativo
Ctrl+Alt+R	annulla il confronto
Ctrl+Alt+1	visualizza tutti gli elementi
Ctrl+Alt+2	visualizza solo gli elementi aggiunti, il rapporto mostrerà gli elementi presenti nel rapporto attuale
Ctrl+Alt+3	visualizza solo gli elementi rimossi, il rapporto mostrerà gli elementi presenti nel rapporto precedente
Ctrl+Alt+4	visualizza solo gli elementi sostituiti (compresi i file)
Ctrl+Alt+5	visualizza solo le differenze tra i rapporti
Ctrl+Alt+C	visualizza il confronto
Ctrl+Alt+N	visualizza il rapporto attuale
Ctrl+Alt+P	apre il rapporto precedente

Varie

F1	visualizza la guida
Alt+F4	chiude il programma
Alt+Maiusc+F4	chiude il programma senza chiedere
Ctrl+I	statistiche registro

5.5.2.3 Confronta

La funzione Confronta consente di mettere a confronto due rapporti esistenti. Il risultato di questa funzione è una serie di elementi non comuni ai due rapporti. È la soluzione adatta se si desidera rilevare le modifiche nel sistema ed è un utile strumento per individuare l'attività del codice dannoso.

Dopo l'avvio, l'applicazione crea un nuovo rapporto, visualizzato in una nuova finestra. Andare a **File** > **Salva rapporto** per salvare un rapporto in un file. I file di rapporto possono essere aperti e visualizzati in un secondo momento. Per aprire un rapporto esistente, accedere a **File** > **Apri rapporto**. Nella finestra principale del programma, ESET SysInspector visualizza sempre un rapporto alla volta.

Il confronto tra due rapporti offre il vantaggio di visualizzare un rapporto attualmente attivo e uno salvato in un file. Per confrontare due rapporti, utilizzare l'opzione **File** > **Confronta rapporto** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Nel rapporto comparativo saranno visualizzate solo le differenze tra i due.

NOTA: se si mettono a confronto due file di rapporto, selezionando **File** > **Salva rapporto** e salvandoli in un file ZIP, verranno salvati entrambi i file. Se si apre il file in un secondo momento, i rapporti contenuti verranno automaticamente messi a confronto.

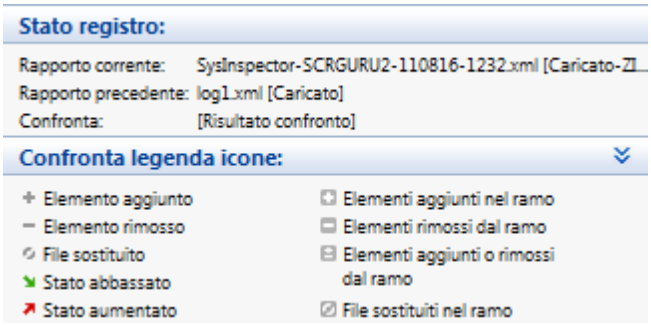
Accanto agli elementi visualizzati, ESET SysInspector mostra i simboli che identificano le differenze tra i rapporti confrontati.

Gli elementi contrassegnati con – si trovano solo nel rapporto attivo e non erano presenti nel rapporto comparativo aperto. Gli elementi contrassegnati con + erano presenti solo nel rapporto aperto e non sono presenti in quello attivo.

Descrizione di tutti i simboli che possono essere visualizzati accanto agli elementi:

- + nuovo valore, non presente nel rapporto precedente
- la sezione della struttura contiene nuovi valori
- – valore rimosso, presente solo nel rapporto precedente
- la sezione della struttura contiene i valori rimossi
- il valore/file è stato modificato
- la sezione della struttura contiene valori/file modificati
- il livello di rischio è diminuito/era più alto nel precedente rapporto
- il livello di rischio è aumentato/era più basso nel precedente rapporto

Nella sezione di descrizione visualizzata nell'angolo in basso a sinistra vengono descritti tutti i simboli e mostrati i nomi dei rapporti confrontati.



Qualsiasi rapporto comparativo può essere salvato in un file e aperto successivamente.

Esempio

Generare e salvare un rapporto, registrando le informazioni originali sul sistema, in un file denominato previous.xml. Dopo aver effettuato le modifiche al sistema, aprire ESET SysInspector e attendere che venga eseguito un nuovo rapporto. Salvarlo in un file denominato current.xml.

Al fine di rilevare le modifiche tra i due rapporti, andare a **File** > **Confronta rapporti**. Il programma crea un rapporto comparativo che visualizza solo le differenze tra i due.

È possibile ottenere lo stesso risultato utilizzando la seguente opzione della riga di comando:

SysIsnpector.exe current.xml previous.xml

5.5.3 Parametri della riga di comando

ESET SysInspector supporta la generazione di rapporti dalla riga di comando con i seguenti parametri:

/gen	genera un rapporto direttamente dalla riga di comando senza eseguire l'interfaccia utente
/privacy	genera un rapporto escludendo informazioni riservate
/zip	archivia il rapporto risultante direttamente sul disco in un file compresso
/silent	nasconde la barra di avanzamento della generazione del rapporto
/help, /?	visualizza informazioni sui parametri della riga di comando

Esempi

Per caricare un rapporto specifico direttamente nel browser, digitare: SysInspector.exe "c:\clientlog.xml"
Per generare un rapporto in un percorso corrente, digitare: SysInspector.exe /gen
Per generare un rapporto in una cartella specifica, digitare: SysInspector.exe /gen="c:\folder\"
Per generare un rapporto in un file/percorso specifico, digitare: SysInspector.exe /gen="c:\folder\mynewlog.xml"
Per generare un rapporto escludendo le informazioni sensibili direttamente in un file compresso, digitare: SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip
Per confrontare due rapporti, digitare: SysInspector.exe "current.xml" "original.xml"

NOTA: Se il nome di un file/cartella contiene uno spazio vuoto, è necessario inserirlo tra virgolette.

5.5.4 Script di servizio

Lo script di servizio è uno strumento utile per i clienti che utilizzano ESET SysInspector in quanto consente di rimuovere facilmente gli oggetti indesiderati dal sistema.

Lo script di servizio consente all'utente di esportare l'intero rapporto di ESET SysInspector o le parti selezionate. Al termine dell'esportazione, è possibile selezionare gli oggetti indesiderati da eliminare. È quindi possibile eseguire il rapporto modificato per eliminare gli oggetti contrassegnati.

Lo script di servizio è adatto agli utenti avanzati che hanno già esperienza nella diagnostica dei problemi del sistema. Le modifiche effettuate da persone non qualificate potrebbero causare danni al sistema operativo.

Esempio

Se si sospetta che il computer sia infettato da un virus non rilevato dal programma antivirus, attenersi alle seguenti istruzioni dettagliate:

- Eseguire ESET SysInspector per generare un nuovo snapshot del sistema.
- Selezionare il primo elemento della sezione sulla sinistra (nella struttura ad albero), premere Shift ed evidenziare l'ultimo elemento per selezionarli tutti.
- Fare clic con il pulsante destro del mouse sugli oggetti selezionati e scegliere l'opzione del menu contestuale **Esporta sezioni selezionate a script di servizio**.
- Gli oggetti selezionati verranno esportati in un nuovo rapporto.
- Questo è il passaggio più importante dell'intera procedura: aprire il nuovo rapporto e cambiare l'attributo - in + per tutti gli oggetti che si desidera rimuovere. Fare attenzione a non contrassegnare file/oggetti importanti del sistema operativo.
- Aprire ESET SysInspector, fare clic su **File** > **Esegui script di servizio** e immettere il percorso dello script.
- Fare clic su **OK** per eseguire lo script.

5.5.4.1 Generazione dello script di servizio

Per generare uno script, fare clic con il pulsante destro del mouse su qualsiasi voce della struttura del menu (nel riquadro a sinistra) nella finestra principale di ESET SysInspector. Selezionare l'opzione **Esporta tutte le sezioni a script di servizio** o l'opzione **Esporta sezioni selezionate a script di servizio** nel menu contestuale.

NOTA: non è possibile esportare lo script di servizio quando vengono confrontati due rapporti.

5.5.4.2 Struttura dello script di servizio

Nella prima riga dell'intestazione dello script sono disponibili informazioni sulla versione del motore (ev), sulla versione dell'interfaccia utente (gv) e sulla versione del rapporto (lv). Questi dati possono essere utilizzati per tenere traccia delle possibili variazioni nel file XML che genera lo script e prevenire eventuali incoerenze durante l'esecuzione. Non modificare questa parte dello script.

La restante parte del file è suddivisa in sezioni in cui è possibile modificare gli elementi (indicare quelli che saranno elaborati dallo script). È possibile contrassegnare gli elementi da elaborare sostituendo il carattere "-" davanti a un elemento con il carattere "+". Le sezioni dello script sono separate tra loro mediante una riga vuota. A ogni sezione viene assegnato un numero e un titolo.

01) Processi in esecuzione

Questa sezione contiene un elenco di tutti i processi in esecuzione nel sistema. Ogni processo è identificato mediante il proprio percorso UNC e, successivamente, dal rispettivo codice hash CRC16 tra asterischi (*).

Esempio:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Nell'esempio, è stato selezionato un processo, module32.exe (contrassegnato dal carattere "+"). Il processo terminerà all'esecuzione dello script.

02) Moduli caricati

In questa sezione sono contenuti i moduli di sistema attualmente in uso.

Esempio:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Nell'esempio, il modulo khbekhb.dll è stato contrassegnato con "+". All'esecuzione dello script, i processi che eseguono tale modulo specifico verranno riconosciuti e interrotti.

03) Connessioni TCP

Questa sezione contiene informazioni sulle connessioni TCP esistenti.

Esempio:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

All'esecuzione dello script, verrà individuato il proprietario del socket nelle connessioni TCP contrassegnate e il socket verrà interrotto, liberando le risorse del sistema.

04) Endpoint UDP

Questa sezione contiene informazioni sugli endpoint UDP esistenti.

Esempio:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

All'esecuzione dello script, verrà isolato il proprietario del socket sugli endpoint UDP contrassegnati e il socket verrà interrotto.

05) Voci server DNS

Questa sezione contiene informazioni sulla configurazione del server DNS corrente.

Esempio:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

All'esecuzione dello script, le voci del server DNS contrassegnate verranno rimosse.

06) Voci importanti del Registro di sistema

Questa sezione contiene informazioni su importanti voci del Registro di sistema.

Esempio:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

All'esecuzione dello script, le voci contrassegnate verranno eliminate, ridotte a valori a 0 byte o ripristinate sui valori predefiniti. L'azione da eseguire su una particolare voce dipende dalla categoria della voce stessa e dal valore principale nel Registro di sistema specifico.

07) Servizi

In questa sezione sono riportati i servizi registrati all'interno del sistema.

Esempio:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

All'esecuzione dello script, i servizi contrassegnati e i relativi servizi dipendenti verranno interrotti e disinstallati.

08) Driver

In questa sezione sono riportati i driver installati.

Esempio:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando si esegue lo script, i driver selezionati verranno arrestati. Tenere presente che alcuni driver non possono essere arrestati.

09) File critici

Questa sezione contiene informazioni sui file critici per il corretto funzionamento del sistema operativo.

Esempio:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Gli elementi selezionati saranno eliminati o ripristinati sui valori originali.

5.5.4.3 Esecuzione degli script di servizio

Contrassegnare tutti gli elementi desiderati, quindi salvare e chiudere lo script. Eseguire lo script modificato direttamente dalla finestra principale di ESET SysInspector selezionando l'opzione **Esegui script di servizio** dal menu File. All'apertura di uno script, verrà visualizzato il seguente messaggio: **Eseguire lo script di servizio "%Scriptname%"?** Dopo aver confermato, verrà visualizzato un altro messaggio per segnalare che lo script di servizio che si sta cercando di eseguire non è stato firmato. Fare clic su **Esegui** per avviare lo script.

Verrà visualizzata una finestra di dialogo per confermare la corretta esecuzione dello script.

Se lo script è stato eseguito solo parzialmente, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio è stato eseguito parzialmente. Visualizzare il rapporto degli errori?** Selezionare **Sì** per visualizzare un rapporto completo degli errori in cui sono indicate le operazioni non eseguite.

Se lo script non viene riconosciuto, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio selezionato non è firmato. L'esecuzione di script sconosciuti o non firmati potrebbe causare seri danni ai dati nel computer. Eseguire lo script e le azioni?** Ciò potrebbe essere causato da incoerenze all'interno dello script (intestazione danneggiata, titolo della sezione danneggiato, linea vuota tra le sezioni e così via). È possibile riaprire il file script e correggere gli errori all'interno dello script o creare un nuovo script di servizio.

5.5.5 Domande frequenti

ESET SysInspector richiede privilegi di amministratore per l'esecuzione?

Anche se per eseguire ESET SysInspector non sono necessari privilegi di amministratore, alcune informazioni raccolte possono essere visualizzate solo da un account amministratore. Eseguendo il programma come utente standard o utente con restrizioni, si raccoglieranno meno informazioni sull'ambiente operativo in uso.

ESET SysInspector crea un file di rapporto?

ESET SysInspector può creare un file di rapporto della configurazione del proprio computer. Per salvarlo, selezionare **File** > **Salva rapporto** dal menu principale. I rapporti vengono salvati nel formato XML. Per impostazione predefinita, i file vengono salvati nella directory %USERPROFILE%\Documenti\, con una convenzione di denominazione file "SysInpsector-%COMPUTERNAME%-AAMMGG-HHMM.XML". Se preferibile, è possibile modificare la posizione e il

nome del file di rapporto prima di salvarlo.

Come si visualizza il file di rapporto di ESET SysInspector?

Per visualizzare un file di rapporto creato da ESET SysInspector, eseguire il programma e selezionare **File** > **Apri rapporto** dal menu principale. È anche possibile trascinare i file di rapporto all'interno dell'applicazione ESET SysInspector. Se è necessario consultare frequentemente i file di rapporto di ESET SysInspector, è consigliabile creare un collegamento sul Desktop al file SYSINSPECTOR.EXE, quindi sarà sufficiente trascinare i file di rapporto sopra di esso per poterli visualizzare. Per motivi di protezione, in Windows Vista/7 la funzione di trascinamento della selezione tra finestre con differenti autorizzazioni di protezione potrebbe non essere disponibile.

È disponibile una specifica per il formato del file di rapporto? E per quanto riguarda un SDK?

Attualmente non è disponibile né una specifica per il file di rapporto né un SDK, in quanto il programma è ancora in fase di sviluppo. Dopo il rilascio del programma, potrebbero essere forniti sulla base dei commenti e delle richieste dei clienti.

In che modo ESET SysInspector valuta il rischio di un determinato oggetto?

Nella maggior parte dei casi, ESET SysInspector assegna livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ogni oggetto e quindi ne valutano le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso). Nel riquadro di spostamento a sinistra, le sezioni sono colorate sulla base del livello di rischio più elevato di un oggetto al loro interno.

Un livello di rischio "6 - Sconosciuto (rosso)" significa che un oggetto è pericoloso?

Le valutazioni di ESET SysInspector non garantiscono che un oggetto sia dannoso. Questa affermazione dovrebbe essere eseguita da un esperto di sicurezza. ESET SysInspector è progettato per fornire una rapida valutazione agli esperti di sicurezza, in modo da informarli su quali oggetti del sistema potrebbero richiedere una loro ulteriore analisi in presenza di comportamento anomalo.

Perché ESET SysInspector si collega a Internet quando viene avviato?

Al pari di molte applicazioni, ESET SysInspector è provvisto di firma digitale, un certificato che garantisce la pubblicazione del software da parte di ESET e l'assenza di alterazione dello stesso. Al fine di verificare il certificato, il sistema operativo contatta un'autorità di certificazione per verificare l'identità dell'autore del software. Si tratta di una procedura comune eseguita su tutti i programmi con firma digitale eseguiti in Microsoft Windows.

Cos'è la tecnologia Anti-Stealth?

La tecnologia Anti-Stealth assicura un efficace rilevamento di rootkit.

Se il sistema viene attaccato da codice dannoso che si comporta come un rootkit, l'utente può essere esposto al rischio di perdita o furto dei dati. In assenza di uno strumento speciale anti-rootkit, è quasi impossibile rilevarli.

Perché a volte i file contrassegnati come "Firmati da MS", hanno contemporaneamente un "Nome aziendale" differente?

Quando si cerca di identificare la firma digitale di un file eseguibile, ESET SysInspector verifica innanzitutto se nel file è incorporata una firma digitale. Se viene trovata una firma digitale, il file verrà convalidato usando tali informazioni. Se la firma digitale non viene trovata, ESI inizia a ricercare il file CAT corrispondente (Catalogo di protezione - %systemroot% \system32\catroot) contenente informazioni sul file eseguibile elaborato. Nel caso in cui dovesse trovare il file CAT appropriato, nel processo di convalida del file eseguibile verrà applicata la firma digitale di tale file CAT.

Per tale motivo, a volte i file contrassegnati come "Firmati da MS", hanno contemporaneamente un "Nome aziendale" differente.

Esempio:

Windows 2000 include l'applicazione HyperTerminal nel percorso C:\Programmi\Windows NT. Il file eseguibile dell'applicazione principale non è firmato a livello digitale, ma ESET SysInspector lo contrassegna come file firmato da Microsoft. Ciò dipende da un riferimento in C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE} \sp4.cat che punta a C:\Programmi\Windows NT\hypertrm.exe (il principale file eseguibile dell'applicazione HyperTerminal) e sp4.cat è firmato a livello digitale da Microsoft.

5.5.6 ESET SysInspector come componente di ESET Endpoint Security

Per aprire la sezione ESET SysInspector in ESET Endpoint Security, fare clic su **Strumenti** > **ESET SysInspector**. Il sistema di gestione della finestra di ESET SysInspector è simile a quello dei rapporti di scansione del computer o delle attività pianificate. Tutte le operazioni con gli snapshot del sistema (crea, visualizza, confronta, rimuovi ed esporta) sono accessibili con pochi clic.

La finestra di ESET SysInspector contiene informazioni di base sugli snapshot creati, quali data e ora di creazione, breve commento, nome dell'utente che ha creato lo snapshot e stato dello snapshot.

Per eseguire il confronto, la creazione o l'eliminazione degli snapshot, utilizzare i pulsanti corrispondenti nella parte inferiore della finestra di ESET SysInspector. Quelle opzioni sono disponibili anche dal menu contestuale. Per visualizzare lo snapshot di sistema selezionato, utilizzare l'opzione **Mostra** del menu contestuale. Per esportare lo snapshot selezionato in un file, fare clic con il pulsante destro del mouse, quindi selezionare **Esporta...**.

Di seguito viene fornita una descrizione dettagliata delle opzioni disponibili:

- **Confronta** - Consente di confrontare due rapporti esistenti. È idonea se si desidera rilevare le modifiche tra il rapporto attuale e uno precedente. Per utilizzare questa opzione, selezionare due snapshot da mettere a confronto.
- **Crea...** - Consente di creare un nuovo record. È prima necessario inserire un breve commento sul record. Per visualizzare lo stato di avanzamento della procedura di creazione dello snapshot (relativamente allo snapshot in corso di generazione), fare riferimento alla colonna **Stato**. Tutti gli snapshot completati sono contrassegnati dallo stato **Creato**.
- **Elimina/Elimina tutto** - Consente di rimuovere le voci dall'elenco.
- **Esporta...** - Salva la voce selezionata in un file XML (anche in una versione compressa).

5.6 ESET SysRescue

ESET SysRescue è un'utilità che consente di creare un disco di avvio contenente una delle soluzioni ESET Security: può essere ESET NOD32 Antivirus, ESET Smart Security o anche uno dei prodotti per server. Il vantaggio principale offerto da ESET SysRescue consiste nel fatto che la soluzione ESET Security viene eseguita indipendentemente dal sistema operativo che la ospita e, al tempo stesso, dispone dell'accesso diretto al disco e all'intero file system. Ciò consente di rimuovere infiltrazioni che non sarebbe stato possibile eliminare in una situazione ordinaria, ad esempio durante l'esecuzione del sistema operativo.

5.6.1 Requisiti minimi

ESET SysRescue è eseguibile su Microsoft Windows Preinstallation Environment (Windows PE) versione 2.x, basato su Windows Vista.

Windows PE è incluso nel pacchetto gratuito Windows Automated Installation Kit (Windows AIK) e pertanto deve essere installato prima di procedere alla creazione di ESET SysRescue (http://go.eset.eu/AIK). A seguito del supporto della versione a 32 bit di Windows PE, è necessario usare un pacchetto di installazione della soluzione ESET Security a 32 bit durante la creazione di ESET SysRescue sui sistemi a 64 bit. ESET SysRescue supporta Windows AIK 1.1 e versioni successive.

NOTA: poiché Windows AIK è superiore a 1 GB, per un download lineare è necessaria una connessione Internet ad alta velocità.

ESET SysRescue è disponibile nelle soluzioni ESET Security 4.0 e versioni successive.

Sistemi operativi supportati

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 con KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 con KB926044
- Windows XP Service Pack 3

5.6.2 Come creare un CD di ripristino

Per avviare la procedura guidata di ESET SysRescue, fare clic su **Start** > **Programmi** > **ESET** > **ESET Endpoint Security** > **ESET SysRescue**.

Innanzitutto, la procedura guidata rileva la presenza di Windows AIK e di un dispositivo adatto alla creazione di un supporto di avvio. Se Windows AIK non è installato nel computer, se è danneggiato o installato in modo errato, la procedura guidata consentirà di installarlo o di inserire il percorso della cartella di Windows AIK (http://go.eset.eu/AIK).

NOTA: poiché Windows AIK è superiore a 1 GB, per un download lineare è necessaria una connessione Internet ad alta velocità.

Al passaggio successivo, selezionare il supporto di destinazione in cui si desidera posizionare ESET SysRescue.

5.6.3 Selezione delle destinazioni

Oltre che su CD/DVD/USB, è possibile scegliere di salvare ESET SysRescue anche in un file ISO. Successivamente, sarà possibile masterizzare l'immagine ISO su CD/DVD o utilizzarla in altro modo (ad esempio in ambienti virtuali quali VmWare o Virtualbox).

Se è stato selezionato il dispositivo USB come supporto di destinazione, è possibile che su alcuni computer non sia possibile eseguire l'avvio. Alcune versioni del BIOS possono riportare problemi di comunicazione con Boot manager (ad esempio, con Windows Vista) e durante l'avvio vengono visualizzati i seguenti messaggi di errore:

```
file : \boot\bcd
stato : 0xc000000e
informazioni : si è verificato un errore durante il tentativo di leggere i dati della configurazione di avvi
```

Nel caso si verificasse questo tipo di errore, si consiglia di selezionare un supporto CD anziché USB.

5.6.4 Impostazioni

Prima di avviare la creazione di ESET SysRescue, nell'ultimo passaggio della procedura di installazione guidata di ESET SysRescue vengono visualizzati i parametri di compilazione. Tali parametri possono essere modificati facendo clic sul pulsante **Cambia...**. Le opzioni disponibili includono:

- Cartelle
- Antivirus ESET
- Avanzate
- Protocollo Internet
- Supporto USB di avvio (quando è selezionato il supporto USB di destinazione)
- Masterizzazione (quando è selezionata l'unità CD/DVD di destinazione)

Il pulsante **Crea** rimane inattivo se non viene specificato alcun pacchetto di installazione MSI o se nel computer non viene installata alcuna soluzione ESET Security. Per selezionare un pacchetto di installazione, fare clic sul pulsante **Cambia** e andare alla scheda **ESET Antivirus**. Se non si inseriscono nome utente e password (**Cambia** > **ESET Antivirus**), il pulsante **Crea** non è disponibile.

5.6.4.1 Cartelle

La **Cartella temporanea** è una cartella di lavoro per i file richiesti per la compilazione di ESET SysRescue.

Cartella ISO è una cartella in cui vengono salvati, al termine della compilazione, i file ISO.

L'elenco presente in questa scheda riporta tutti i dischi di rete locali e mappati insieme allo spazio disponibile residuo. Se alcune cartelle si trovano in un disco che non dispone di spazio sufficiente, si consiglia di selezionare un disco alternativo che disponga di maggiore spazio. In caso contrario, è possibile che la compilazione si interrompa in modo anomalo a causa della mancanza di spazio libero su disco.

Applicazioni esterne - Consente di specificare programmi aggiuntivi che saranno eseguiti o installati dopo il riavvio da un supporto ESET SysRescue.

Includi applicazioni esterne - Consente di aggiungere programmi esterni alla compilazione di ESET SysRescue.

Cartella selezionata - Cartella in cui si trovano i programmi da aggiungere al disco di ESET SysRescue.

5.6.4.2 Antivirus ESET

Per la creazione di ESET SysRescue CD, è possibile selezionare due origini di file ESET utilizzabili dal compilatore.

Cartella ESS/EAV - File già contenuti nella cartella da cui la soluzione ESET Security è stata installata nel computer.

File MSI - Vengono utilizzati i file contenuti nel programma di installazione di MSI.

È quindi possibile scegliere di aggiornare il percorso dei file (nup). Normalmente è consigliabile scegliere l'opzione predefinita **Cartella ESS/EAV/File MSI**. In alcuni casi, è possibile scegliere una **Cartella di aggiornamento** personalizzata, ad esempio per utilizzare una versione precedente o più recente del database delle firme antivirali.

È possibile utilizzare una delle due origini seguenti di nome utente e password:

ESS/EAV installato - Il nome utente e la password saranno copiati dalla soluzione ESET Security attualmente installata.

Da utente - Verranno utilizzati il nome utente e la password immessi nelle caselle di testo corrispondenti.

NOTA: La soluzione ESET Security su ESET SysRescue CD viene aggiornata da Internet o dalla soluzione ESET Security installata nel computer sul quale è in esecuzione ESET SysRescue CD.

5.6.4.3 Impostazioni avanzate

La scheda **Avanzate** consente di ottimizzare ESET SysRescue CD rispetto alle dimensioni della memoria del computer. Selezionare **576 MB o più** per scrivere il contenuto del CD nella memoria operativa (RAM). Se si seleziona **meno di 576 MB**, durante l'esecuzione di WinPE sarà sempre possibile accedere al CD di ripristino.

Nella sezione **Driver esterni** è possibile immettere i driver per gli hardware specifici utilizzati dall'utente (in genere, la scheda di rete). Sebbene WinPE sia basato su Windows Vista SP1, che supporta una vasta gamma di hardware, talvolta l'hardware non viene riconosciuto. È quindi necessario aggiungere il driver manualmente. Esistono due modi per introdurre il driver nella compilazione di ESET SysRescue: manualmente (mediante il pulsante **Aggiungi**) e automaticamente (mediante il pulsante **Ricerca aut.**). In caso di inserimento manuale, è necessario selezionare il percorso del file .inf corrispondente (è inoltre necessario che in questa cartella sia presente anche il file *.sys applicabile). In caso di introduzione automatica, il driver viene rilevato automaticamente nel sistema operativo di un determinato computer. Si consiglia di utilizzare l'inserimento automatico unicamente se ESET SysRescue viene utilizzato su un computer che dispone della stessa scheda di rete utilizzata dal computer in cui è stato creato ESET SysRescue CD. Durante la creazione, il driver di ESET SysRescue viene introdotto nella compilazione in modo tale che l'utente non debba cercarlo in seguito.

5.6.4.4 Protocollo Internet

Questa sezione consente di configurare le impostazioni di rete di base e le connessioni predefinite di ESET SysRescue.

Selezionare **Indirizzo IP privato automatico** per ottenere l'indirizzo IP automaticamente dal server DHCP (Dynamic Host Configuration Protocol).

In alternativa, questa connessione di rete può utilizzare un indirizzo IP specificato a livello manuale, anche noto come indirizzo IP statico. Selezionare **Personalizzato** per configurare le impostazioni IP appropriate. Se si seleziona questa opzione, è necessario specificare un **Indirizzo IP** e, per le connessioni LAN e Internet ad alta velocità, una **Maschera subnet**. In **Server DNS preferito** e **Server DNS alternativo**, digitare gli indirizzi del server DNS primario e secondario.

5.6.4.5 Supporto USB di avvio

Se è stato selezionato il dispositivo USB come supporto di destinazione, è possibile selezionare uno dei supporti USB disponibili nella scheda **Supporto USB di avvio** (nel caso siano presenti più dispositivi USB).

Selezionare il **Dispositivo** di destinazione appropriato dove sarà installato ESET SysRescue.

Avviso: durante la creazione di ESET SysRescue, il supporto USB selezionato verrà formattato. Tutti i dati sul supporto verranno cancellati.

Se si seleziona l'opzione **Formattazione rapida**, la formattazione rimuove tutti i file dalla partizione ma non esegue il controllo dei disco alla ricerca di settori errati. Usare questa opzione se il supporto USB è stato precedentemente formattato e si è certi che non sia danneggiato.

5.6.4.6 Masterizza

Se il supporto di destinazione selezionato è CD/DVD, è possibile specificare parametri aggiuntivi di masterizzazione nella scheda **Masterizza**.

Elimina file ISO - Selezionare questa opzione per eliminare il file ISO temporaneo dopo la creazione di ESET SysRescue CD.

Eliminazione attivata - Consente di selezionare le opzioni per l'eliminazione rapida e completa.

Dispositivo di masterizzazione - Selezionare l'unità da utilizzare per la masterizzazione.

Attenzione: questa è l'opzione predefinita. Se viene utilizzato un CD/DVD riscrivibile, tutti i dati in esso contenuti verranno eliminati.

La sezione Supporto contiene informazioni sul supporto nel dispositivo CD/DVD in uso.

Velocità di masterizzazione - Selezionare la velocità desiderata dal menu a discesa. Quando si seleziona la velocità di masterizzazione è necessario tener conto delle capacità del dispositivo di masterizzazione e del tipo di CD/DVD utilizzati.

5.6.5 Utilizzo di ESET SysRescue

Affinché il CD/DVD/USB di ripristino funzioni in maniera ottimale, è necessario avviare il computer dal supporto ESET SysRescue. È possibile modificare la priorità di avvio nel BIOS. In alternativa, è possibile utilizzare il menu di avvio durante l'inizializzazione del computer. In genere si utilizzano i tasti F9 o F12 a seconda della versione della scheda madre/BIOS in uso.

Dopo l'avvio dal supporto di avvio, la soluzione ESET Security viene inizializzata. Poiché ESET SysRescue viene utilizzato solo in situazioni specifiche, l'utilizzo di alcuni moduli di protezione e funzioni del programma disponibili nella versione standard della soluzione ESET Security non è richiesto. L'elenco di tali funzioni e moduli si limita alle operazioni di **Controllo computer**, **Aggiorna** e alcune sezioni in **Configurazione** La funzionalità più importante di ESET SysRescue è la capacità di aggiornare il database delle firme antivirali. Prima di avviare un controllo del computer, è pertanto consigliabile eseguire un aggiornamento del programma.

5.6.5.1 Utilizzo di ESET SysRescue

Si supponga che i computer nella rete siano stati infettati da un virus che modifica i file eseguibili (EXE). La soluzione ESET Security è in grado di pulire tutti i file infetti ad eccezione di explorer.exe, che non può essere pulito neanche in modalità sicura. Ciò dipende dal fatto che anche explorer.exe, in qualità di uno dei processi Windows essenziali, viene lanciato in modalità sicura. La soluzione ESET Security non riuscirebbe ad eseguire alcuna azione sul file che rimarrebbe quindi infettato.

In questo tipo di scenario, è possibile usare ESET SysRescue per risolvere il problema. ESET SysRescue non richiede l'utilizzo di alcun componente del sistema operativo che lo ospita ed è pertanto in grado di elaborare (pulire, eliminare) qualsiasi file sul disco.

6. Glossario

6.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

6.1.1 Virus

Un virus è un pezzo di codice dannoso che è pre-incorporato o viene aggiunto ai file esistenti nel computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro. Il termine "virus" viene spesso utilizzato in maniera errata per indicare qualsiasi tipo di minaccia. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

I virus attaccano principalmente i file eseguibili e i documenti. In breve, un virus funziona nel seguente modo: dopo aver eseguito un file infetto, il codice dannoso viene chiamato ed eseguito prima dell'esecuzione dell'applicazione originale. Un virus può infettare qualsiasi file sul quale l'utente corrente dispone dei diritti di scrittura.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché sono in grado di eliminare deliberatamente i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

Se il computer è stato infettato da un virus e non è possibile rimuoverlo, inviarlo ai laboratori ESET ai fini di un esame accurato. In alcuni casi, i file infetti possono essere modificati a un livello tale da impedirne la pulizia. In questo caso, è necessario sostituire i file con una copia non infetta.

6.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite la rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di propagarsi autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore o persino pochi minuti dal rilascio. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

6.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di minacce che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli così a eseguirli.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- **Downloader** - Programmi dannosi in grado di scaricare altre minacce da Internet.
- **Dropper** - Programmi dannosi in grado di installare sui computer compromessi altri tipi di malware.
- **Backdoor** - Programmi dannosi che comunicano con gli autori degli attacchi remoti, consentendo loro di ottenere l'accesso al computer e assumerne il controllo.
- **Keylogger** (registratore delle battute dei tasti) - Un programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli autori degli attacchi remoti.
- **Dialer** - Programmi dannosi progettati per connettersi a numeri con tariffe telefoniche molto elevate anziché ai provider dei servizi Internet dell'utente. È quasi impossibile che un utente noti che è stata creata una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre meno frequentemente.

Se sul computer in uso viene rilevato un trojan horse, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

6.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli autori degli attacchi su Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per non essere rilevate dal software antivirus: nascondono i processi, i file e i dati del Registro di sistema di Windows. Per tale motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per bloccare i rootkit, sono disponibili due livelli di rilevamento:

1. Quando tentano di accedere a un sistema. Non sono ancora presenti e pertanto sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).
2. Quando sono nascosti dal normale testing. Gli utenti di ESET Endpoint Security hanno il vantaggio di poter utilizzare la tecnologia Antistealth che è in grado di rilevare ed eliminare anche i rootkit attivi.

6.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità (advertising-supported software). Rientrano in questa categoria i programmi che visualizzano materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenenti pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono ai loro sviluppatori di coprire i costi di sviluppo delle applicazioni che, in genere, sono molto utili.

L'adware non è di per sé pericoloso, anche se gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento e registrazione, al pari dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non vengono installati senza adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

6.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è legato al fatto che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware sono frequentemente accoppiati a versioni gratuite di un programma creato dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, è consigliabile eliminarlo in quanto è molto probabile che contenga codice dannoso.

6.1.7 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET Endpoint Security offre la possibilità di rilevare tali minacce.

Applicazioni potenzialmente pericolose è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

6.1.8 Applicazioni potenzialmente indesiderate

Le **applicazioni potenzialmente indesiderate** (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- Nuove finestre mai visualizzate in precedenza (popup, annunci pubblicitari)
- Attivazione ed esecuzione di processi nascosti
- Maggiore utilizzo delle risorse del sistema
- Modifiche dei risultati di ricerca
- Applicazioni che comunicano con server remoti.

6.2 Tipi di attacchi remoti

Esistono molte tecniche particolari che consentono agli autori degli attacchi di compromettere i sistemi remoti. Tali tecniche sono suddivise in diverse categorie.

6.2.1 Attacchi DoS (Denial of Service)

DoS, acronimo di Denial of Service (ovvero negazione del servizio), è un tentativo di rendere un computer o una rete non disponibile agli utenti destinati. Le comunicazioni fra utenti con tale problema vengono bloccate e non possono più essere eseguite in modo efficace. In genere, è necessario riavviare i computer esposti ad attacchi DoS. In caso contrario, potrebbero non funzionare correttamente.

Nella maggior parte dei casi, gli obiettivi sono i server Web, allo scopo di renderli non disponibili agli utenti per un determinato periodo di tempo.

6.2.2 Poisoning del DNS

Attraverso il poisoning DNS (Domain Name Server), gli hacker possono ingannare il server DNS di qualsiasi computer facendo credere che i dati fasulli forniti siano legittimi e autentici. Le false informazioni vengono memorizzate nella cache per un determinato periodi di tempo, consentendo agli autori degli attacchi informatici di riscrivere le risposte DNS degli indirizzi IP. Di conseguenza, gli utenti che tentano di accedere a siti Web su Internet scaricheranno virus o worm nel computer, anziché i contenuti originali.

6.2.3 Attacchi worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. I worm di rete sfruttano le vulnerabilità di diverse applicazioni. Grazie alla disponibilità di Internet, possono diffondersi in tutto il mondo entro poche ore dal loro rilascio, e, in alcuni casi, perfino entro pochi minuti.

La maggior parte degli attacchi worm (Sasser, SqlSlammer) può essere evitata utilizzando le impostazioni di protezione predefinite del firewall, oppure bloccando le porte non protette e inutilizzate. È inoltre essenziale aggiornare il sistema operativo con le patch di protezione più recenti.

6.2.4 Controllo porta

La scansione porta può essere utilizzata per individuare le porte del computer aperte su un host di rete. Uno scanner di porte è un software progettato per rilevare tali porte.

La porta di un computer è un punto virtuale che gestisce i dati in entrata e in uscita: un elemento strategico dal punto di vista della sicurezza. In una rete di grandi dimensioni, le informazioni raccolte dagli scanner di porta possono contribuire a identificare le potenziali vulnerabilità. Tale uso è legittimo.

Tuttavia, la scansione delle porte viene spesso utilizzata dagli hacker nel tentativo di compromettere la sicurezza. Per prima cosa, gli hacker inviano pacchetti a ogni porta. A seconda del tipo di risposta, è possibile stabilire quali sono le porte in uso. La scansione in sé non causa danni, ma occorre tenere presente che questa attività può rivelare le potenziali vulnerabilità e consente agli autori degli attacchi di assumere il controllo dei computer remoti.

Si consiglia agli amministratori di rete di bloccare tutte le porte inutilizzate e proteggere quelle in uso dagli accessi non autorizzati.

6.2.5 Desincronizzazione TCP

La desincronizzazione TCP è una tecnica utilizzata negli attacchi Hijacking TCP. È avviata da un processo in cui il numero sequenziale dei pacchetti in entrata è diverso dal numero sequenziale atteso. I pacchetti con un numero sequenziale inatteso vengono ignorati (o salvati nel buffer, se sono presenti nella finestra della comunicazione corrente).

Nella desincronizzazione, entrambi gli endpoint di comunicazione ignorano i pacchetti ricevuti. Questo è il momento in cui gli autori degli attacchi remoti sono in grado di infiltrarsi e fornire pacchetti con un numero di sequenza corretto. Gli autori degli attacchi sono persino in grado di manipolare o modificare la comunicazione.

Lo scopo degli attacchi Hijacking è interrompere le comunicazioni server-client o peer-to-peer. Molti attacchi possono essere evitati utilizzando l'autenticazione per ciascun segmento TCP. È inoltre opportuno utilizzare le configurazioni consigliate per i dispositivi di rete in uso.

6.2.6 SMB Relay

SMBRelay e SMBRelay2 sono programmi speciali in grado di infliggere attacchi ai computer remoti. Questi programmi si avvalgono del protocollo di condivisione file SMB (Server Message Block) sovrapposto su NetBIOS. Se un utente condivide una cartella o una directory all'interno della LAN, è molto probabile che utilizzi questo protocollo di condivisione file.

Nell'ambito della comunicazione della rete locale, vengono scambiate password hash.

SMBRelay riceve una connessione sulle porte UDP 139 e 445, inoltra i pacchetti scambiati dal client e dal server e li modifica. Dopo aver eseguito la connessione e l'autenticazione, il client viene disconnesso. SMBRelay crea un nuovo indirizzo IP virtuale. È possibile accedere al nuovo indirizzo utilizzando il comando "net use \\192.168.1.1". L'indirizzo può quindi essere utilizzato da qualsiasi funzione di rete di Windows. SMBRelay inoltra la comunicazione del protocollo SMB tranne che per la negoziazione e l'autenticazione. Gli autori dell'attacco remoti possono utilizzare l'indirizzo IP purché il computer client sia connesso.

SMBRelay2 funziona in base agli stessi principi di SMBRelay, tranne per il fatto che utilizza i nomi NetBIOS anziché gli indirizzi IP. Entrambi sono in grado di infliggere attacchi di tipo MITM (man-in-the-middle). Questi attacchi consentono agli autori degli attacchi remoti di leggere, inserire e modificare i messaggi scambiati tra due endpoint di comunicazione senza essere notati. I computer esposti a tali attacchi spesso smettono di rispondere o si riavviano inaspettatamente.

Per evitare gli attacchi, si consiglia di utilizzare password o chiavi di autenticazione.

6.2.7 Attacchi ICMP

ICMP (Internet Control Message Protocol) è un protocollo Internet molto diffuso e ampiamente utilizzato. Viene utilizzato principalmente dai computer in rete per inviare diversi messaggi di errore.

Gli autori degli attacchi informatici in remoto tentano di sfruttare i punti deboli del protocollo ICMP. Il protocollo ICMP è stato progettato per la comunicazione unidirezionale che non prevede l'autenticazione. Questo consente agli autori degli attacchi informatici in remoto di sferrare i cosiddetti attacchi DoS (Denial of Service) o attacchi che consentono a utenti non autorizzati di accedere ai pacchetti in ingresso e in uscita.

Esempi tipici di attacchi ICMP includono attacchi ping flood, ICMP_ECHO flood e smurf. I computer esposti ad attacchi ICMP risultano notevolmente più lenti (ciò è rilevabile su tutte le applicazioni che utilizzano Internet) e presentano problemi di connessione a Internet.

6.3 E-mail

L'e-mail o electronic mail è una moderna forma di comunicazione che presenta numerosi vantaggi. È flessibile, veloce e diretta e ha svolto un ruolo cruciale nella proliferazione di Internet all'inizio degli anni novanta.

Purtroppo, a causa dell'elevato livello di anonimità, i messaggi e-mail e Internet lasciano ampio spazio ad attività illegali come lo spam. Lo spamming include annunci pubblicitari non desiderati, hoax e proliferazione di software dannoso o malware. Ad aumentare ulteriormente i disagi e i pericoli è il fatto che i costi di invio dello spamming sono minimi e gli autori dispongono di numerosi strumenti per acquisire nuovi indirizzi e-mail. Il volume e la varietà dello spamming ne rende inoltre estremamente difficoltoso il monitoraggio. Maggiore è il periodo di utilizzo dell'indirizzo e-mail, più elevata sarà la possibilità che finisca in un database per motori di spamming. Di seguito sono riportati alcuni suggerimenti per la prevenzione di messaggi e-mail indesiderati:

- Se possibile, evitare di pubblicare il proprio indirizzo e-mail su Internet
- Fornire il proprio indirizzo e-mail solo a utenti considerati attendibili
- Se possibile, non utilizzare alias comuni. Maggiore è la complessità degli alias, minore sarà la probabilità che vengano rilevati
- Non rispondere a messaggi di spam già recapitati nella posta in arrivo
- Quando si compilano moduli su Internet, prestare particolare attenzione a selezionare opzioni quali "Sì, desidero ricevere informazioni".
- Utilizzare indirizzi e-mail "specifici", ad esempio uno per l'ufficio, uno per comunicare con gli amici e così via
- Cambiare di tanto in tanto l'indirizzo e-mail
- Utilizzare una soluzione antispam

6.3.1 Pubblicità

La pubblicità su Internet è una delle forme di pubblicità in maggior crescita. I vantaggi principali dal punto di vista del marketing sono i costi ridotti e un livello elevato di immediatezza. I messaggi vengono inoltre recapitati quasi immediatamente. Molte società utilizzano strumenti di marketing via e-mail per comunicare in modo efficace con i clienti attuali e potenziali.

Questo tipo di pubblicità è legittimo, perché si potrebbe essere interessati a ricevere informazioni commerciali su determinati prodotti. Molte società inviano tuttavia messaggi di contenuto commerciale non desiderati. In questi casi, la pubblicità tramite e-mail supera il limite e diventa spam.

La quantità di messaggi e-mail non desiderati diventa così un problema e non sembra diminuire. Gli autori di messaggi e-mail non desiderati tentano spesso di mascherare i messaggi spam come messaggi legittimi.

6.3.2 Hoax: truffe e bufale

Un hoax è un messaggio contenente informazioni non veritiere diffuso su Internet che viene in genere inviato via e-mail e tramite strumenti di comunicazione come ICQ e Skype. Il messaggio stesso è in genere una burla o una leggenda metropolitana.

Gli hoax virus tentano di generare paura, incertezza e dubbio (FUD, Fear, Uncertainty and Doubt) nei destinatari, inducendoli a credere che nei relativi sistemi è presente un "virus non rilevabile" in grado di eliminare file e recuperare password o di eseguire altre attività dannose.

Alcuni hoax richiedono ai destinatari di inoltrare messaggi ai loro contatti, aumentandone così la diffusione. Esistono hoax via cellulare, richieste di aiuto, offerte di denaro dall'estero e così via. Spesso è impossibile determinare l'intento dell'autore del messaggio.

È molto prababile che i messaggi che invitano ad essere inoltrati a tutti i propri conoscenti siano hoax. Su Internet sono presenti molti siti Web in grado di verificare l'autenticità di un messaggio e-mail. Prima di inoltrarlo, effettuare una ricerca in Internet per qualsiasi messaggio si sospetti essere hoax.

6.3.3 Phishing

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni confidenziali). Lo scopo è quello di ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.

Di norma, l'accesso viene ricavato tramite l'invio di messaggi e-mail che imitano quelli di una persona o società affidabile (istituto finanziario, compagnia di assicurazioni). Il messaggio e-mail sembra autentico e presenta immagini e contenuti che possono indurre a credere che provenga effettivamente da un mittente affidabile. Tali messaggi chiedono all'utente, con vari pretesti (verifica dati, operazioni finanziarie), di immettere alcuni dati personali: numeri di conto bancario o nomi utente e password. Tali dati, se inviati, possono essere rubati e utilizzati in modo illegale.

Le banche, le compagnie di assicurazioni e altre società legittime non chiederanno mai di rivelare nomi utente e password in messaggi e-mail non desiderati.

6.3.4 Riconoscimento messaggi spam

In genere, esistono alcuni indicatori che consentono di identificare i messaggi spam (e-mail non desiderate) nella cassetta postale. Un messaggio può essere considerato un messaggio spam se soddisfa almeno alcuni dei criteri riportati di seguito.

- L'indirizzo del mittente non appartiene a nessuno degli utenti presenti nell'elenco dei contatti.
- Agli utenti viene offerta una grossa somma di denaro, purché si impegnino tuttavia ad anticipare una piccola somma di denaro.
- Viene chiesto di immettere con vari pretesti (verifica di dati, operazioni finanziarie) alcuni dati personali, quali numero di conto bancario, nome utente, password e così via
- È scritto in una lingua straniera.
- Viene chiesto di acquistare un prodotto a cui non si è interessati. Se tuttavia si decide di acquistarlo, è consigliabile verificare che il mittente del messaggio sia un fornitore attendibile (contattare il produttore originale)
- Alcuni termini contengono errori di ortografia nel tentativo di aggirare il filtro di spam, ad esempio "vaigra" invece di "viagra" e così via

6.3.4.1 Regole

Nell'ambito delle soluzioni antispam e dei client e-mail, le regole sono strumenti per manipolare le funzioni e-mail. Sono composte da due parti logiche:

1. Condizione (ad esempio, messaggio in arrivo da un determinato indirizzo)
2. Azione (ad esempio, eliminazione del messaggio, spostamento in una cartella specificata)

Il numero e la combinazione di regole varia a seconda della soluzione antispam. Queste regole rappresentano misure contro i messaggi di spam (e-mail indesiderate). Esempi tipici:

- 1. Condizione: un messaggio e-mail in arrivo contiene alcune parole generalmente inserite nei messaggi di spam
  2. Azione: eliminare il messaggio
- 1. Condizione: un messaggio e-mail in arrivo contiene un allegato con estensione .exe
  2. Azione: eliminare l'allegato e recapitare il messaggio alla casella di posta
- 1. Condizione: un messaggio e-mail in arrivo è stato inviato dal datore di lavoro dell'utente
  2. Azione: spostare il messaggio nella cartella "Lavoro"

Si consiglia di utilizzare una combinazione di regole nei programmi antispam per semplificare l'amministrazione e filtrare più efficacemente i messaggi di spam.

6.3.4.2 Whitelist

In generale, una whitelist è un elenco di voci o di persone accettate a cui è stata concessa l'autorizzazione di accesso. Il termine "whitelist di posta" definisce un elenco di contatti da cui l'utente desidera ricevere messaggi. Tali whitelist sono basate su parole chiave ricercate negli indirizzi e-mail, nei nomi di domini o negli indirizzi IP.

Se una whitelist funziona in "modalità di esclusività", i messaggi provenienti da qualsiasi altro indirizzo, dominio o indirizzo IP non verranno ricevuti. Se una whitelist non è esclusiva, tali messaggi non verranno eliminati ma solo filtrati in altro modo.

Una whitelist si basa sul principio opposto di quello di una blacklist. Le whitelist sono relativamente facili da mantenere, molto di più rispetto alle blacklist. Si consiglia di utilizzare sia la whitelist che la blacklist per filtrare più efficacemente i messaggi di spam.

6.3.4.3 Blacklist

In genere, una blacklist è un elenco di persone o elementi non accettati o vietati. Nel mondo virtuale, è una tecnica che consente di accettare messaggi provenienti da tutti gli utenti non presenti in questo elenco.

Esistono due tipi di blacklist: quelle create dall'utente all'interno della propria applicazione antispam e molte blacklist di tipo professionale, aggiornate regolarmente e create da istituzioni specializzate che sono disponibili su Internet.

È essenziale usare le blacklist per bloccare lo spamming in modo efficace. Tali elenchi sono tuttavia difficili da gestire perché ogni giorno si presentano nuovi elementi da bloccare. È pertanto consigliabile utilizzare sia whitelist che blacklist per filtrare in modo più efficace lo spamming.

6.3.4.4 Controllo lato server

Il controllo lato server è una tecnica che consente di identificare spamming di massa in base al numero di messaggi ricevuti e alle reazioni degli utenti. Ogni messaggio lascia una "impronta" digitale univoca in base al suo contenuto. Il numero ID univoco non fornisce alcuna informazione in merito al contenuto del messaggio e-mail. Due messaggi identici avranno impronte identiche, mentre messaggi diversi avranno impronte diverse.

Se un messaggio viene contrassegnato come spam, l'impronta corrispondente viene inviata al server. Se il server riceve più impronte identiche (che corrispondono a un determinato messaggio di spam), l'impronta viene memorizzata nel database di impronte di spam. Durante il controllo dei messaggi in arrivo, il programma invia le impronte dei messaggi al server. Il server restituisce informazioni sulle impronte corrispondenti ai messaggi già contrassegnati dagli utenti come spam.